PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-160003
(43)Date of publication of application : 12.06.2001

(51)Int.Cl. G06F 12/14
G06F 13/00
G06F 17/60
G10K 15/02
H04N 7/08
H04N 7/081
H04N 7/173

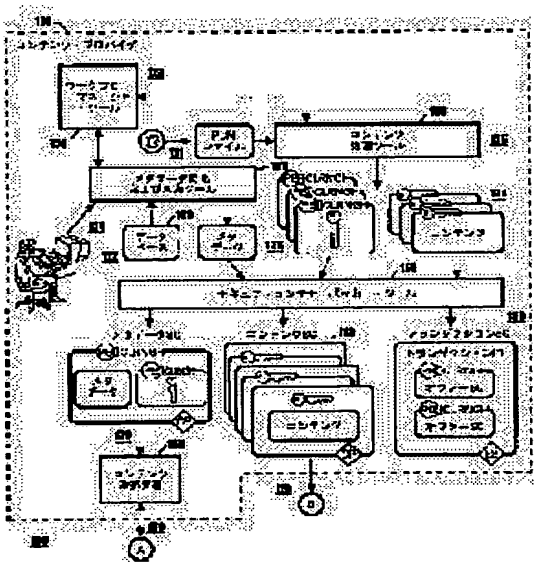
(21)Application number : 2000-279877
(22)Date of filing : 14.09.2000

(71)Applicant : INTERNATL BUSINESS MACH CORP <IBM>
(72)Inventor : DORACK JR JOHN J

(30)Priority
Priority number : 1999 397419 Priority date : 17.09.1999 Priority country : US

(54) METHOD AND DEVICE FOR UNIQUELY IDENTIFYING CUSTOMER PURCHASE IN ELECTRONIC DISTRIBUTION SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a system for tracing the use of digital contents on a user device.
SOLUTION: A content site distributes digital contents via a computer-readable medium to a user. The content site relates an unique content identifier with the related contents. An electronic store connected with a network sells a license for reproducing the digital content data to the user. The license includes the unique item identifier for uniquely identifying at least one item in the transaction. Then, a content, player which receives the content data given the license from the network, is used for the reproduction of the content data given the license. The content player prepares a purchase identifier, based on the mathematical combination of the content identifier, the transaction identifier, and the item identifier.



LEGAL STATUS
[Date of request for examination] 14.09.2000
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

書誌

(19)【発行国】日本国特許庁(JP)
(12)【公報種別】公開特許公報(A)
(11)【公開番号】特開2001－160003(P2001－160003A)
(43)【公開日】平成13年6月12日(2001. 6. 12)
(54)【発明の名称】電子配布システム内で顧客購入を一意に識別するための方法および装置
(51)【国際特許分類第7版】

G06F	12/14	320
	13/00	540
	17/60	142
		302
G10K	15/02	
H04N	7/08	
	7/081	
	7/173	640

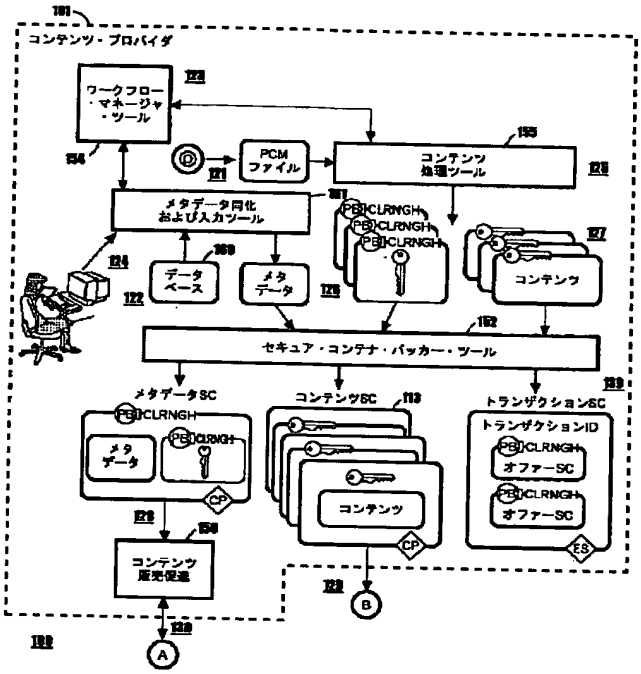
【FI】

G06F	12/14	320 E
	13/00	540 S
	17/60	142
		302 E
G10K	15/02	
H04N	7/173	640 Z
	7/08	Z

【審査請求】有
【請求項の数】20
【出願形態】OL
【全頁数】82
(21)【出願番号】特願2000－279877(P2000－279877)
(22)【出願日】平成12年9月14日(2000. 9. 14)
(31)【優先権主張番号】09／397419
(32)【優先日】平成11年9月17日(1999. 9. 17)
(33)【優先権主張国】米国(US)
(71)【出願人】
【識別番号】390009531
【氏名又は名称】インターナショナル・ビジネス・マシーンズ・コーポレーション
【氏名又は名称原語表記】INTERNATIONAL BUSINESS MASCHINES CORPORATION
【住所又は居所】アメリカ合衆国10504、ニューヨーク州 アーモンク (番地なし)
(72)【発明者】
【氏名】ジョン・ジェイ・ドラク・ジュニア
【住所又は居所】アメリカ合衆国33428 フロリダ州ボカ・ラトン エス・ダブリュー62番 アベニュー22238
(74)【代理人】
【識別番号】100086243
【弁理士】
【氏名又は名称】坂口 博 (外2名)

要約

(57)【要約】
【課題】 ユーザ装置上でディジタル・コンテンツの使用を追跡するためのシステム。
【解決手段】 コンテンツ・サイトが、コンピュータ可読媒体を介してディジタル・コンテンツをユーザに配布する。コンテンツ・サイトは、関連するコンテンツに一意のコンテンツ識別子を関連付ける。ネットワークに結合された電子商店が、ディジタル・コンテンツ・データを再生するためのライセンスをユーザに売る。ライセンスには、トランザクションを一意に識別するための一意のトランザクション識別子が含まれ、ライセンスには、トランザクション内の少なくとも1つの項目を一意に識別するための一意の項目識別子が含まれる。ライセンスを交付されたコンテンツ・データをネットワークから受信するコンテンツ・プレイヤが、ライセンスを交付されたコンテンツ・データの再生に使用される。コンテンツ・プレイヤは、コンテンツ識別子、トランザクション識別子、および項目識別子の数学的組合せに基づいて購入識別子を作る。



請求の範囲

【特許請求の範囲】
【請求項1】ディジタル・コンテンツ・プレイヤ上でディジタル・コンテンツをユニークに識別する方法であって、コンテンツ・プロバイダから受信した前記ディジタル・コンテンツをユニークに識別する第1識別子を受信するステップと、前記ディジタル・コンテンツをそれによって受信したトランザクションをユニークに識別する第2識別子を受信するステップと、前記ディジタル・コンテンツをそれによって受信したトランザクション内の項目をユニークに識別する第3識別子を受信するステップと、前記第1識別子、前記第2識別子、および前記第3識別子の数学的組合せに基づいて、第4ユニーク識別子を作るステップとを含む、ディジタル・コンテンツをユニークに識別する方法。
【請求項2】前記作るステップが、前記第1識別子、前記第2識別子、および前記第3識別子の連結に基づいて第4ユニーク識別子を作ることを含む、請求項1に記載のディジタル・コンテンツをユニークに識別する方法。
【請求項3】前記第2識別子を受信するステップが、前記ディジタル・コンテンツを売る商店からユニークな識別子を受信することを含む、請求項1に記載のディジタル・コンテンツをユニークに識別する方法。
【請求項4】前記第3識別子を受信するステップが、前記ディジタル・コンテンツを売る商店から、前記ディジタル・コンテンツがそれによって受信されたトランザクションをユニークに識別するユニークな識別子を受信することを含む、請求項3に記載のディジタル・コンテンツをユニークに識別する方法。
【請求項5】使用条件を含む前記ディジタル・コンテンツに前記第4ユニーク識別子を関連付けるステップと、前記ディジタル・コンテンツを再生する前に、前記第4ユニーク識別子をインデクシングすることによって前記使用条件を再検討するステップとをさらに含む、請求項1に記載のディジタル・コンテンツをユニークに識別する方法。
【請求項6】第4ユニーク識別子を作る前記ステップが、第4ユニーク識別子への許可されないアクセスを防ぐために、耐タンパ環境で前記第4ユニーク識別子を作ることを含む、請求項1に記載のディジタル・コンテンツをユニークに識別する方法。
【請求項7】ユーザ装置上でディジタル・コンテンツの使用を追跡するシステムであって、コンピュータ可読媒体上でディジタル・コンテンツをユーザに配布する複数のコンテンツ・サイトであって、前記ディジタル・コンテンツが、それに関連付けられたユニークなコンテンツ識別子を含む、複数のコンテンツ・サイトと、ディジタル・コンテンツ・データを再生するライセンスをユーザに与える複数の電子商店であって、各電子商店が、ネットワークに結合され、前記ライセンスが、トランザクションをユニークに識別するユニークなトランザクション識別子を含み、前記ライセンスが、前記トランザクション内の少なくとも1つの項目をユニークに識別するユニークな項目識別子を含む、複数の電子商店と、コンテンツ・データを再生する複数のコンテンツ・プレイヤであって、各ディジタル・コンテンツ・プレイヤが、前記ユーザのうちの1つによってライセンスを交付された前記ディジタル・コンテンツ・データを前記ネットワークから受信し、前記コンテンツ・プレイヤが、前記コンテンツ識別子、前記トランザクション識別子、および前記項目識別子の数学的組合せに基づいて購入識別子を作る、複数のコンテンツ・プレイヤとを含む、ユーザ装置上でディジタル・コンテンツの使用を追跡するシステム。
【請求項8】前記数学的組合せが、連結である、請求項7に記載のユーザ装置上でディジタル・コンテンツの使用を追跡するシステム。
【請求項9】前記コンテンツ・プレイヤが、耐タンパ環境を含み、前記購入識別子が、それへの許可されないアクセスを防ぐために、前記耐タンパ環境内で作られる、請求項7に記載のユーザ装置上でディジタル・コンテンツの使用を追跡するシステム。
【請求項10】ディジタル・コンテンツをユニークに識別するディジタル・コンテンツ・プレイヤであって、コンテンツ・プロバイダから受信した前記ディジタル・コンテンツをユニークに識別する第1識別子を受信する手段と、前記ディジタル・コンテンツがそれによって受信されたトランザクションをユニークに識別する第2識別子を受信する手段と、前記ディジタル・コンテンツがそれによって受信されたトランザクション内の項目をユニークに識別する第3識別子を受信する手段と、前記第1識別子、前記第2識別子、および前記第3識別子の数学的組合せに基づいて第4ユニーク識別子を作る手段とを含む、ディジタル・コンテンツをユニークに識別するディジタル・コンテンツ・プレイヤ。
【請求項11】前記作る手段が、前記第1識別子、前記第2識別子、および前記第3識別子の連結に基づいて第4ユニーク識別子を作ることを含む、請求項10に記載のディジタル・コンテンツをユニークに識別するディジタル・コンテンツ・プレイヤ。
【請求項12】前記第2識別子を受信する手段が、前記ディジタル・コンテンツを売る商店からユニークな識別子を受信することを含

む、請求項10に記載のディジタル・コンテンツをユニークに識別するディジタル・コンテンツ・プレイヤ。
【請求項13】前記第3識別子を受信する手段が、前記ディジタル・コンテンツを売る商店から、前記ディジタル・コンテンツがそれによって受信されたトランザクションをユニークに識別するユニークな識別子を受信することを含む、請求項10に記載のディジタル・コンテンツをユニークに識別するディジタル・コンテンツ・プレイヤ。
【請求項14】使用条件を含む前記ディジタル・コンテンツに前記第4ユニーク識別子を関連付ける手段と、前記ディジタル・コンテンツを再生する前に、前記第4ユニーク識別子をインデクシングすることによって前記使用条件を再検討する手段とをさらに含む、請求項10に記載のディジタル・コンテンツをユニークに識別するディジタル・コンテンツ・プレイヤ。
【請求項15】ディジタル・コンテンツ・プレイヤ上でディジタル・コンテンツをユニークに識別するプログラム命令を含むコンピュータ可読媒体であって、コンテンツ・プロバイダから受信した前記ディジタル・コンテンツをユニークに識別する第1識別子を受信するプログラム命令と、前記ディジタル・コンテンツをそれによって受信したトランザクションをユニークに識別する第2識別子を受信するプログラム命令と、前記ディジタル・コンテンツをそれによって受信したトランザクション内の項目をユニークに識別する第3識別子を受信するプログラム命令と、前記第1識別子、前記第2識別子、および前記第3識別子の数学的組合せに基づいて、第4ユニーク識別子を作るプログラム命令とを含む、コンピュータ可読媒体。
【請求項16】前記作るプログラム命令が、前記第1識別子、前記第2識別子、および前記第3識別子の連結に基づいて第4ユニーク識別子を作ることを含む、請求項15に記載のコンピュータ可読媒体。
【請求項17】前記第2識別子を受信するプログラム命令が、前記ディジタル・コンテンツを売る商店からユニークな識別子を受信することを含む、請求項15に記載のコンピュータ可読媒体。
【請求項18】前記第3識別子を受信するプログラム命令が、前記ディジタル・コンテンツを売る商店から、前記ディジタル・コンテンツがそれによって受信されたトランザクションをユニークに識別するユニークな識別子を受信することを含む、請求項17に記載のコンピュータ可読媒体。
【請求項19】使用条件を含む前記ディジタル・コンテンツに前記第4ユニーク識別子を関連付けるプログラム命令と、前記ディジタル・コンテンツを再生する前に、前記第4ユニーク識別子をインデクシングすることによって前記使用条件を再検討するプログラム命令とをさらに含む、請求項15に記載のコンピュータ可読媒体。
【請求項20】第4ユニーク識別子を作る前記プログラム命令が、第4ユニーク識別子への許可されないアクセスを防ぐために、耐タンパ環境で前記第4ユニーク識別子を作ることを含む、請求項15に記載のコンピュータ可読媒体。

詳細な説明

【発明の詳細な説明】
【0001】
【発明の属する技術分野】開示される発明は、広義には、電子商取引の分野に関し、具体的には、印刷媒体、フィルム、ゲーム、および音楽などのディジタル資産の、インターネットおよびワールド・ワイド・ウェブなどのグローバル通信ネットワークを介する安全な配布および権利管理のためのシステムおよび関連ツールに関する。
【0002】
【従来の技術】関連出願の相互参照本特許出願は、1998年8月13日出願の米国特許出願第09／133519号明細書の一部継続出願である1998年10月22日出願の米国特許出願第09／177096号明細書の一部継続出願である。以前の米国特許出願第09／177096号明細書の開示全体が、参照によって本明細書に組み込まれる。
【0003】音楽、フィルム、コンピュータ・プログラム、絵、ゲーム、および他のコンテンツなどのディジタル資産を配布するための、インターネットなどのグローバル配布システムの使用が、成長を続けている。それと同時に、貴重なディジタル・コンテンツの所有者および発行者は、複数の理由から、ディジタル資産の配布へのインターネットの使用を採用するのが遅れていた。理由の1つは、所有者が、ディジタル・コンテンツの許可されないコピーまたは海賊行為を恐れていることである。ディジタル・コンテンツの電子配布は、海賊行為に対する複数の障壁を取り除く。電子配布によって取り除かれる障壁の1つが、有形の記録可能媒体そのもの（たとえばディスケットまたはCD－ROM）の必要である。有形の媒体へのディジタル・コンテンツのコピーは、多くの場合に空白テープまたは記録可能CDについては1ドル未満であるとはいえ、金がかかる。しかし、電子配布の場合には、有形の媒体はもはや不要である。コンテンツが電子的に配布されるので、有形の媒体のコストは要因ではなくなる。第2の障壁は、コンテンツ自体のフォーマットすなわち、アナログ形式で格納されたコンテンツとディジタル形式で格納されたコンテンツの対比である。アナログ形式で格納されたコンテンツ、たとえば印刷された絵は、写真複写によって複製される時に、コピーはオリジナルより品質が下がる。コピーの後続のコピーのそれぞれを、世代と称する場合があるが、各世代は、オリジナルより品質が劣る。この品質劣化は、絵がディジタル的に格納される時には存在しない。各コピーおよびコピーのすべての世代が、オリジナルと同様に明瞭で新鮮なものとなり得る。電子的なコンテンツ配布およびインターネットを介する広範囲でのコンテンツ配布の非常に低いコストと組み合わされた完全なディジタル・コピーの組合せ効果によって、海賊行為と許可されないコピーの配布がかなり簡単になる。わずかなキーストロークで、海賊は、数百個または数千個のディジタル・コンテンツの完全なコピーを、インターネットを介して送信することができる。したがって、電子的に配布されるディジタル資産の保護およびセキュリティを確保する必要が存在する。
【0004】ディジタル・コンテンツのプロバイダは、コンテンツ所有者の権利を保護する、ディジタル・コンテンツ用の保護されたグローバル配布システムを確立することを望んでいる。ディジタル・コンテンツ配布システムの確立に伴う問題には、ディジタル・コンテンツ電子配布、権利管理、および資産保護のためのシステムを開発することが含まれる。電子的に配布されるディジタル・コンテンツには、印刷媒体、フィルム、ゲーム、プログラム、テレビジョン、マルチメディア、および音楽などのコンテンツが含まれる。
【0005】電子配布システムの展開によって、ディジタル・コンテンツ・プロバイダに、即時の販売報告作成および電子調整を介する支払のすばやい清算を達成する能力ならびに、コンテンツの再配布を介する2次収入源を得る能力がもたらされる。電子ディジタル・コンテンツ配布システムは、物理的な在庫不足または返品によって影響されないので、ディジタル・コンテンツ・プロバイダおよび小売業者は、コスト削減および改善された粗利益を実現することができる。ディジタル・コンテンツ・プロバイダは、よりよく時間を制限された在庫放出のための、新規の配布チャンネルを促進するか、既存の配布チャネルを増補することができる。電子配布システムからのトランザクシン・データは、消費者の購入パターンに関する情報の取得ならびに電子マーケティング・プログラムおよび販売促進に対する即時フィードバックの提供に使用することができる。これらの目標を満たすために、ディジタル・コンテンツ・プロバイダが、ディジタル資産の保護を保証し測定を行いながら、広範囲のユーザおよび会社がディジタル・コンテンツを入手できるようにする電子配布モデルを使用することの必要が存在する。
【0006】real audio、AT＆T社のA2B、Liquid Audio Pro Corp.社のLiquid AudioPro、Audio Soft社のCity Music Networkその他などのディジタル・コンテンツ用の他の市販電子配布システムは、保護された電子ネットワークおよび保護されない電子ネットワークを介するディジタル・データの伝送を提供する。保護された電子ネットワークの使用によって、ディジタル・コンテンツを広範囲の聴衆に配布するというディジタル・コンテンツ・プロバイダの必要条件が大幅に削減される。インターネットおよびウェブなどの保護されないネットワークを使用することによって、ディジタル・コンテンツが、暗号の使用を介するなど、保護された形でエンドユーザに到達することが可能になる。しかし、暗号化されたディジタル・コンテンツが、エンドユーザの計算機上で暗号解読された後は、そのディ

ジタル・コンテンツは、許可されない再配布のためにエンドユーザが簡単に使用できるようになる。したがって、ディジタル資産の保護を提供し、ディジタル・コンテンツが消費者および会社に配布された後であってもコンテンツ・プロバイダの権利が保護されることを保証する、セキュア・ディジタル・コンテンツ電子配布システムの必要が存在する。したがって、安全な配布、ライセンス交付許可、およびディジタル資産の使用量の制御を可能にする権利管理の必要が存在する。

【0007】ディジタル・コンテンツの所有者が電子配布の採用に遅れていたもう1つの理由は、彼らが、既存の配布のチャネルを維持し、育成することを望んでいることである。ほとんどのコンテンツ所有者は、小売業者を介して販売する。音楽市場では、これらの米国の小売業者に、Tower Records、Peaches、Blockbuster、Circuit Cityその他が含まれる。これらの小売業者の多くは、インターネット・ユーザがインターネットを介して選択を行い、選択したものをエンドユーザにメールで送らせることを可能にするウェブ・サイトを有する。音楽ウェブ・サイトの例には、@tower、Music Boulevard、およびColumbia Houseが含まれる。電子配布を使用すると、小売り店が、特にウェブ上で、お互いからそれ自体を差別化し、コンテンツ所有者からそれ自体を差別化する能力が奪われる可能性がある。したがって、絵、ゲーム、音楽、プログラム、およびビデオなどの電子コンテンツの小売業者に、電子配布を介して音楽を販売する時にお互いおよびコンテンツ所有者からそれ自体を差別化する方法を提供する必要が存在する。

【0008】コンテンツ所有者は、電子商店などの配布サイトを介する電子配布のためにディジタル・コンテンツを準備する。インターネット上または他のオンライン・サービスを介する電子商店は、製品オファリングおよび製品販売促進によってお互いからそれ自体を差別化することを求める。従来の商店すなわち、非電子、非オンラインの電子商店類似物は、製品販売促進、製品セールス、製品サンプル、寛大な返品方針、および他の販売促進プログラムを使用して、競争者からそれ自体を差別化する。しかし、コンテンツ・プロバイダがディジタル・コンテンツに対する使用条件を課すオンラインの世界では、電子商店がそれ自体を差別化する能力が、厳しく制限される可能性がある。さらに、使用条件を変更することができる場合であっても、電子商店は、製品を電子的に販売促進し、販売するために、コンテンツ・プロバイダからのディジタル・コンテンツに関連するメタデータを処理するという困難な作業に直面する。電子商店は、メタデータを処理する時に複数の要件を管理する必要がある。第1に、電子商店は、コンテンツ・プロバイダからディジタル・コンテンツに関連するメタデータを受け取る必要がある。多くの場合に、このメタデータの一部が暗号化されて送られる場合があり、したがって、コンテンツ・プロバイダは、暗号化されたコンテンツを解読する機構を作成しなければならない。第2に、電子商店は、コンテンツ・プロバイダからコンテンツを受け取る前か、電子商店がコンテンツを受け取った後のいずれかに、製品のマーケティング、製品の位置付け、およびコンテンツに関する他の販売促進考慮事項を支援するために、コンテンツ・プロバイダからのメタデータをプレビューすることを望む可能性がある。第3に、電子商店は、グラフィックスおよびアーティスト情報などの販売促進材料のために使用されるいくつかのメタデータを抽出する必要がある。しばしば、この販売促進材料が、電子商店によって、そのオンライン販売促進に直接に使用される。第4に、電子商店は、許可された使用条件の一部を変更して、ディジタル・コンテンツの異なるオファリングを作成することによって、お互いからのそれ自体の差別化を望む場合がある。第5に、電子商店は、支払い清算のために電子商店を通過する必要なしに、購入者によって支払調整を自動的に会計調整会社に向けるために、メタデータ内にURLなどのアドレスを挿入するか変更する必要がある場合がある。第6に、電子商店は、使用条件に一致する著作権付きのディジタル・コンテンツの許可される使用に関するライセンスを作成する必要がある場合がある。たとえば、このライセンスでは、ディジタル・コンテンツの限られた数のコピーを作ることの許可を与えることができる。ライセンスは、与えられる許可の期間および条件を反映するために必要である。

【0009】これらの必要条件のすべてに鑑みて、ディジタル・コンテンツに関係するメタデータを処理するために、多数の電子商店が、これらの必要条件を処理するためにカスタマイズされたソフトウェア・プログラムを作成する。これらのカスタマイズされたソフトウェア・プログラムを作成するのに必要な時間、コスト、およびテストは、大きくなる可能性がある。したがって、これらの必要条件に対する解決策を提供する必要が存在する。

【0010】さらに、ディジタル・コンテンツの所有者が電子配布の採用に遅れていたもう1つの理由は、電子配布のためにコンテンツを準備することの難しさである。現在、コンテンツのプロバイダの多くが、その作品集に数千もしくは数万のタイトルを有する。音楽の例では、コンテンツ所有者が、同時に複数の異なるフォーマット(たとえばCD、テープ、およびミニディスク)で入手可能な単一のマスタ・サウンド・レコーディングを有することが珍しくない。さらに、単一のフォーマットが、特定の配布チャネル用に再マスタリングまたはリミックスされたマスタ・サウンド・レコーディングを有する可能性がある。一例として、ラジオ放送用のミキシングは、ダンス・クラブ・サウンド・トラック用のミキシングと異なる場合があり、これが、一般に入手可能な消費者CDと異なる場合がある。これらの異なるミックスの在庫管理および記録は、重荷になる可能性がある。さらに、マスタ・レコーディングの所有者の多くは、「ベスト・オブ～」などのさまざまな後続のコレクションで、または、映画の音楽サウンド・トラックの編集物または他のコレクションまたは編集物で、古いレコーディングを再発行することがしばしばである。ディジタルに提供されるコンテンツが増えるにつれて、電子配布のためにコンテンツをリミックスし、符号化する必要が増す。多くの場合に、プロバイダは、正しいマスタ・サウンド・レコーディングを選択するための案内役として古いレコーディング・フォーマットを使用する必要があり、これらのサウンド・レコーディングを、電子配布用の公開のために再処理させ、符号化させる。これは、電子配布用の古いサウンド・レコーディングの再公開での支援のために古いフォーマットを使用することを望むコンテンツ・プロバイダの場合に特にそうである可能性がある。プロバイダは、データベースを調べて、タイトル、アーティスト、およびサウンド・レコーディングを照合して、符号化パラメータを設定する。レコーディング集のデータベースを手動で検索するこの処理は、短所がないわけではない。短所の1つは、操作員に手動でデータベースを検索させ、処理パラメータを適当に設定させる必要である。もう1つの短所は、データベースからデータを選択する際の操作員のトランスクリプション・エラーの可能性である。したがって、コンテンツ・プロバイダに、オーディオなどのコンテンツに関して、関連データおよびマスタ・レコーディングを自動的に取り出す方法を提供する必要が存在する。

【0011】コンテンツ所有者は、符号化と称する処理を介して、電子配布のためにディジタル・コンテンツを準備する。符号化には、コンテンツをとり、コンテンツがアナログ・フォーマットで提示される場合にはディジタル化し、コンテンツを圧縮することが含まれる。圧縮の処理によって、伝送または格納されるデータの量が減るので、ディジタル・コンテンツを、より効率的にネットワークを介して伝送でき、記録可能媒体に格納できるようになる。しかし、圧縮は、短所がないわけではない。ほとんどの圧縮は、いくらかの情報の消失が伴い、ロッシイ圧縮と呼ばれる。コンテンツ・プロバイダは、どの圧縮アルゴリズムを使用し、どの圧縮レベルが必要であるかを決定しなければならない。たとえば、音楽では、ディジタル・コンテンツまたは曲は、音楽のジャンルに応じて非常に異なる特性を有する可能性がある。あるジャンルのために選択された圧縮アルゴリズムおよび圧縮レベルが、別のジャンルの音楽には最適の選択でない場合がある。コンテンツ・プロバイダは、圧縮アルゴリズムおよび圧縮レベルのある組合せが、たとえばクラシックなど、音楽のあるジャンルについて非常に良好に動作するが、ヘビー・メタルなどの音楽の別のジャンルについては不満足な結果をもたらすことに気付く可能性がある。さらに、オーディオ・エンジニアは、音楽を等化し、ダイナミック・レンジ調整を行い、他の前処理および処理設定を実行して、符号化される音楽のジャンルが所望の結果を生むようにしなければならないことがしばしばである。ディジタル・コンテンツごとに等化レベル設定およびダイナミック・レンジ設定などの符号化パラメータを必ず手動で設定しなければならないという要件は、重荷になる可能性がある。音楽の例に戻ると、さまざまな音楽ジャンルを含むコレクションを有する音楽のコンテンツ・プロバイダは、符号化される曲または曲の組ごとに、符号化パラメータの所望の組合せを手動で選択しなければならないはずである。したがって、符号化の処理パラメータを手動で選択する必要を克服する必要が存在する。

【0012】コンテンツを圧縮する処理は、特に省略なしの映画などの大きいコンテンツ項目の場合に、大量の専用計算リソースを必要とする可能性がある。圧縮アルゴリズムのプロバイダは、その圧縮技法に関連するさまざまなトレードオフおよび長所を提供す

る。このトレードオフには、コンテンツを圧縮するのに必要な時間および計算リソースの量、オリジナル・コンテンツから達成される圧縮の量、再生に望まれるビット・レート、圧縮されたコンテンツのパフォーマンス品質、および他の要因が含まれる。入力としてマルチメディア・ファイルをとり、進行または状況の中間表示なしで符号化された出力ファイルを生成する符号化プログラムの使用が、問題である。さらに、多くの状況では、他のプログラムが、進行の中間表示のない符号化プログラムを呼び出すかこれを管理するのに使用される。これによって、呼出し側のアプリケーションは、符号化を指定された選択物全体の比率として符号化されたコンテンツの量を示す方法がなくなる。呼出し側プログラムが、同時に複数の異なるプログラムを稼動させるようにスケジューリングしようとする場合には、これが問題になる可能性がある。さらに、コンテンツのバッチが符号化のために選択され、コンテンツ・プロバイダが符号化処理の進行状況を判定したい場合には、これが特に重荷になる可能性がある。したがって、この問題を克服する必要が存在する。

【0013】ディジタル・コンテンツ・プロバイダが、彼らのコンテンツについて電子配布の採用に遅れていたもう1つの理由が、電子配布されたコンテンツ用のエンドユーザ装置でのディジタル・プレイヤを作成するための標準の欠如である。コンテンツ・プロバイダ、電子商店、または電子配布チェーン内の他者は、PCS、セットトップ・ボックス、手持ち装置その他などのさまざまな装置でのカスタマイズされたプレイヤを提供することを望む可能性がある。耐タンパ(耐変更)環境すなわち、再生中のコンテンツへのサード・パーティによる許可されないアクセスを抑止する環境で、ディジタル・コンテンツの解読を処理できるツールの組が必要である。さらに、エンドユーザが、購入されたもの以外の用途のためのコンテンツへのアクセス権を許可されずに、ディジタル・コンテンツのローカル・ライブラリを管理できるようにするためのツールの組が必要である。

【0014】コンテンツ所有者がディジタル・コンテンツの配布に関して直面するもう1つの問題は、購入トランザクションに、同一の一固まりのコンテンツの複数のコピーが含まれる場合である。たとえば、ある顧客が、1つのコピーを作成する権利と共に曲または映画を購入すると仮定する。さらに、この顧客は、コピーを作成する権利を伴わない曲の第2の選択を友人のために購入することを決定した。この曲の購入者にとって、同一の曲の同一のコピーを混同することは簡単である。コンテンツ所有者は、曲のそれぞれの選択、特に同一の曲を追跡することを望むので、これは望ましくない。曲、特に同一の曲を追跡することの望みは、同一の曲のそれぞれの使用条件を追跡しなければならない時にはさらに重要になる。さらに、同一の曲が、多数の異なるコレクションまたは組で公開されることが一般的である。たとえば、同一の曲が、シングル、アルバムまたはCDの一部、グレーテスト・ヒット・コレクションの一部、および、将来にボックス・セットの一部になる場合がある。同一の曲のこれらの異なるリリースのすべてを有すると、追跡が困難になる可能性がある。したがって、これらの問題を克服するために、ディジタル・コンテンツを一意(ユニーク)に追跡する方法およびシステムの必要が存在する。

【0015】ディジタル・コンテンツの保護の背景に関するさらなる情報は、以下の3つの供給源から見つけることができる。URL「http://www.a2bmusic.com/about/papers/musicipp.htm」でオンライン入手可能な、米国ニュージャージー州FlorhamParkのAT&T Labsのレイシー(Jack Lacy)、シュナイダー(James Snyder)、メイハー(David Maher)共著、「Music on the Internet and the Intellectual Property Protection Problem」。URL「http://www.intertrust.com/architecture/stc.html」でオンライン入手可能な、米国カリフォルニア州SunnyvaleのInterTrust Technologies Corp.社のシバート(Olin Sibert)、バーンシュタイン(David Bernstein)、およびウィー(David Van Wie)共著の論文、「Securingthe Content, Not the Wire for Information Commerce」に記載の、DigiBoxと称する、暗号的に保護されたコンテナ。URL「http:///cyptolope.ibm.com/white.htm」でオンライン入手可能なIBM社のホワイト・ペーパー「CryptolopeContainer Technology」である。

【0016】

【発明が解決しようとする課題】本発明の目的は、上で述べた短所を除去し、コンテンツ・データの使用を追跡するためのシステムを提供することである。

【0017】

【課題を解決するための手段】本発明の一実施形態は、ユーザ装置上のディジタル・コンテンツの使用を追跡するシステムを提供する。コンテンツ・サイトが、コンピュータ可読媒体を介してディジタル・コンテンツをユーザに配布する。コンテンツ・サイトは、関連するコンテンツに一意のコンテンツ識別子を関連付ける。ネットワークに結合された電子商店が、ディジタル・コンテンツ・データを再生するライセンスをユーザに販売する。このライセンスには、トランザクションを一意に識別するための一意のトランザクション識別子が含まれ、このライセンスには、トランザクション内の少なくとも1つの項目を一意に識別するための一意の項目識別子が含まれる。ライセンスを交付されたコンテンツ・データをネットワークから受信するコンテンツ・プレイヤが、ライセンスを交付されたコンテンツ・データの再生に使用される。コンテンツ・プレイヤは、コンテンツ識別子、トランザクション識別子、および項目識別子の数学的組合せに基づいて、購入識別子を作る。

【0018】

【発明の実施の形態】読者がこの実施形態の異なる部分をすばやく突きとめるのを支援するために、本明細書の目次を示す。

ト4. 解読1505、圧縮解除1506および再生コンポーネント5. データ管理1502およびライブラリ・アクセス・コンポーネント6. アプリケーション間通信コンポーネント7. その他種々のコンポーネント8. 汎用プレイヤ【0019】I. セキュア・ディジタル・コンテンツ電子配布システムA. システムの概要セキュア・ディジタル・コンテンツ電子配布システムは、エンドユーザのクライアント装置へのディジタル・コンテンツおよびディジタル・コンテンツに関係するコンテンツの安全な配布および権利管理に必要な技術、仕様、ツール、およびソフトウェアを含む技術プラットホームである。エンドユーザ装置には、PCS、セット・トップ・ボックス(IRD)、およびインターネット機器が含まれる。これらの装置は、コンテンツ所有者による許可に従って、コンテンツを外部媒体またはポータブル消費者装置にコピーすることができる。用語「ディジタル・コンテンツ」または単に「コンテンツ」は、絵、映画、ビデオ、音楽、プログラム、マルチメディア、およびゲームを含む、ディジタル・フォーマットで格納された情報およびデータを指す。

【0020】技術プラットホームは、ディジタル・コンテンツが、準備され、2地点間インフラストラクチャおよびブロードキャスト・インフラストラクチャ(ケーブル、インターネット、衛星、および無線など)を介してエンドユーザ装置に保護された形で配布され、ライセンスを交付され、許可されないコピーまたは再生から保護される方法を指定する。さらに、技術プラットホームのアーキテクチャを用いると、ウォーターマーキング、圧縮／符号化、暗号化、および他のセキュリティ・アルゴリズムなどのさまざまな技術の、将来にこれらが開発された時の統合および移植が可能になる。

【0021】セキュア・ディジタル・コンテンツ電子配布システムの基本コンポーネントは、(1)コンテンツ所有者の所有権の保護のための権利管理と、(2)即時の正確な報酬のためのトランザクション測定と、(3)標準に準拠するすべてのプレイヤでの再生のために、コンテンツ・プロバイダがコンテンツを準備し、複数のネットワーク・インフラストラクチャを介する保護された配送を許可することができるようにする、オープンで明確に文書化されたアーキテクチャである。

【0022】1. 権利管理セキュア・ディジタル・コンテンツ電子配布システムの権利管理は、システムのオペレーティング・コンポーネント間に分配された機能の組を介して実施される。その主要な機能には、ライセンスを確保した許可された仲介者または許可されたエンドユーザだけによってコンテンツがロック解除されるようにするライセンス交付許可およびライセンス交付制御と、許可されるコピーの数、再生の回数、ライセンスが有効である時間間隔または期間などの、購入またはライセンスの条件に従うコンテンツ使用の制御および強制とが含まれる。権利管理の副次的な機能は、海賊行為と戦うために、コンテンツの許可されないコピーの出所を識別する手段を使用可能にすることである。

【0023】ライセンス交付許可およびライセンス交付制御は、クリアリングハウス実体およびセキュア・コンテナ(SC)技術の使用を介して実施される。クリアリングハウスは、仲介者またはエンドユーザが、ライセンス交付トランザクションの成功裡の完了の検証の後にコンテンツをロック解除できるようにすることによって、ライセンス交付許可をもたらす。セキュア・コンテナは、暗号化されたコンテンツおよび情報をシステム・コンポーネント間で配布するのに使用される。SCは、暗号、ディジタル署名、およびディジタル証明書を使用して、電子情報およびコンテンツの許可されない傍受または変更に対する保護を提供する、情報またはコンテンツの暗号的担体である。SCを用いると、ディジタル・コンテンツの認証性および保全性の検証も可能になる。これらの権利管理機能の長所は、電子ディジタル・コンテンツ配布インフラストラクチャが、保護されることも信頼されることも必要でないことである。したがって、ウェブおよびインターネットなどのネットワーク・インフラストラクチャを介する伝送が可能になる。これは、コンテンツがセキュア・コンテナ内で暗号化され、その格納および配布が、そのロック解除および使用の制御から分離されているという事実に起因する。解読キーを有するユーザだけが、暗号化されたコンテンツのロックを解除することができ、クリアリングハウスは、許可された適当な使用要求のみについて解読キーを公開する。クリアリングハウスは、未知のまたは許可されない当事者からの偽の要求、またはコンテンツ所有者によって設定されるコンテンツの使用条件に従わない要求を許可しない。さらに、SCが、伝送中に変更(tamper)された場合には、クリアリングハウスのソフトウェアが、SCのコンテンツが破壊または偽造されていると判定し、そのトランザクションを拒絶する。

【0024】コンテンツ使用の制御は、エンドユーザ装置上で稼動するエンドユーザのプレイヤ・アプリケーション195を介して使用可能にされる。このアプリケーションは、許容される2次コピーおよび再生の数を定義するディジタル・コードを、コンテンツのすべてのコピーに埋め込む。ディジタル・ウォーターマーキング技術を使用して、ディジタル・コードを生成し、他のエンドユーザのプレイヤ・アプリケーション195からそのディジタル・コードを隠し、変更の試みに対して抵抗するようにする。代替実施形態では、ディジタル・コードは、単にコンテンツ113に関連する使用条件の一部として保存される。コンテンツ113が、準拠エンドユーザ装置内でアクセスされる時には、エンドユーザのプレイヤ・アプリケーション195が、透かしを読み取って、使用制限を検査し、必要に応じて透かしを更新する。たとえば、コピーの回数を使い果たしたなど、コンテンツの要求された使用が使用条件に従わない場合には、エンドユーザ装置は、その要求を実行しない。

【0025】ディジタル・ウォーターマーキングは、コンテンツの許可されたコピーまたは許可されないコピーの出所を識別する手段も提供する。コンテンツ内の最初の透かしは、コンテンツ所有者を識別し、著作権情報を指定し、地理的配布区域を定義し、他の関連情報を追加するために、コンテンツ所有者によって埋め込まれる。第2の透かしは、コンテンツの購入者(またはライセンス交付を受けた者)とエンドユーザ装置を識別し、購入またはライセンスの条件および日付を指定し、他の関連情報を追加するために、エンドユーザ装置でコンテンツに埋め込まれる。

【0026】透かしは、コンテンツの肝要な部分になるので、コピーが許可されたものであったか否かに無関係に、コピー内に担持される。したがって、ディジタル・コンテンツには、コンテンツがどこにあり、どこから来たかに無関係に、その出所と許可された使用に関する情報が必ず含まれる。この情報を使用して、コンテンツの不正使用と戦うことができる。

【0027】2. 測定その権利管理機能の一部として、クリアリングハウスは、そのクリアリングハウスを介して鍵交換が許可されたすべてのトランザクションの記録を保持する。この記録を用いると、ライセンス交付許可およびオリジナルの使用条件の測定が可能になる。トランザクション記録は、コンテンツ所有者またはコンテンツ・プロバイダ、小売業者、または他者などの、責任のある当事者に、即時にまたは周期的に報告して、トランザクション支払および他の使用の電子調整を促進することができる。

【0028】3. オープン・アーキテクチャセキュア・ディジタル・コンテンツ電子配布システムは、公開された仕様およびインターフェースを有して、市場でのセキュア・ディジタル・コンテンツ電子配布システムの幅広い実施および受入を促進すると同時にコンテンツ所有者の権利保護を維持する、オープン・アーキテクチャである。セキュア・ディジタル・コンテンツ電子配布システムの柔軟性とオープン性によって、さまざまな技術、伝送インフラストラクチャ、および装置が市場に配送されるにつれて、時と共にセキュア・ディジタル・コンテンツ電子配布システムが進歩することも可能になる。

【0029】このアーキテクチャは、コンテンツの性質およびそのフォーマットに関してオープンである。オーディオ、プログラム、マルチメディア、ビデオ、または他の種類のコンテンツの配布が、このアーキテクチャによってサポートされる。コンテンツは、ディジタル音楽用のリニアPCMなどのネイティブ・フォーマット、または、フィルタリング、圧縮、またはプリエンファシス／デエンファシスその他などの追加の前処理または符号化によって達成されるフォーマットとすることができる。このアーキテクチャは、さまざまな暗号化技法およびウォーターマーキング技法に対してオープンである。このアーキテクチャでは、コンテンツの異なる種類およびフォーマットを受け入れ、新技術が現れた時にそれを導入または採用できるようにするために、特定の技法を選択することができる。この柔軟性によって、コンテンツ・プロバイダは、セキュア・ディジタル・コンテンツ電子配布システム内でのデータ圧縮、暗号化、およびフォーマッティングに使用する技術を選択し、進化させることができる。

【0030】このアーキテクチャは、異なる配布ネットワークおよび配布モデルに対してもオープンである。このアーキテクチャは、低速のインターネット接続または高速の衛星ネットワークおよびケーブル・ネットワークを介するコンテンツ配布をサポートし、2地点間モ

デルまたはブロードキャスト・モデルと共に使用することができる。さらに、このアーキテクチャは、低コスト消費者装置を含む広範囲の装置でエンドユーザ装置の機能を実施できるように設計されている。この柔軟性によって、コンテンツ・プロバイダおよび小売業者は、さまざまなサービス・オファリングを介して仲介者またはエンドユーザにコンテンツを提供できるようになり、ユーザが、コンテンツを購入するかライセンスの交付を受け、それを再生し、さまざまな準拠プレイヤ装置で記録することができるようになる。

【0031】B. システムの機能要素ここで図1ないし4を参照すると、本発明によるセキュア・ディジタル・コンテンツ電子配布システム100の概要を示すブロック図が示されている。セキュア・ディジタル・コンテンツ電子配布システム100には、終端間ソリューションを含む複数のビジネス・エレメント(business element)が含まれ、これには、コンテンツ・プロバイダ101またはディジタル・コンテンツ所有者、電子ディジタル・コンテンツ商店103、仲介市場パートナー(図示せず)、クリアリングハウス105、コンテンツ・ホスティング・サイト111、伝送インフラストラクチャ107、およびエンドユーザ装置109が含まれる。これらのビジネス・エレメントのそれぞれが、セキュア・ディジタル・コンテンツ電子配布システム100のさまざまなコンポーネントを使用する。電子的なコンテンツ113の配布に具体的に関係する、これらのビジネス・エレメントおよびシステム・コンポーネントの高水準の説明を以下に示す。

【0032】1. コンテンツ・プロバイダ101コンテンツ・プロバイダ101またはコンテンツ所有者は、オリジナルのコンテンツ113の所有者であるか、さらに配布するために独立のコンテンツ113をパッケージ化することを許可された卸売業者であるか、その両方である。コンテンツ・プロバイダ101は、その権利を直接に利用するか、通常は電子商取引収入に関係するコンテンツ使用料支払の返礼として、コンテンツ113のライセンスを電子ディジタル・コンテンツ商店103または仲介市場パートナー(図示せず)に交付することができる。コンテンツ・プロバイダ101の例には、Sony、Time-Warner、MTV、IBM、Microsoft、Turner、Fox、その他が含まれる。

【0033】コンテンツ・プロバイダ101は、コンテンツ113および関連データを配布用に準備するために、セキュア・ディジタル・コンテンツ電子配布システム100の一部として提供されるツールを使用する。ワーク・フロー・マネージャ・ツール154は、処理されるコンテンツ113をスケジューリングし、コンテンツ113の準備およびパッケージ化のさまざまなステップを通って流れる際にコンテンツ113を追跡して、高品質保証を維持する。用語メタデータは、この文書全体を通じて、コンテンツ113に関連するデータを意味するのに使用され、この実施形態では、コンテンツ113自体を含まない。一例として、曲のメタデータは、曲の題名または曲のクレジットとすることができるが、曲のサウンド・レコーディングではない。コンテンツ113に、サウンド・レコーディングが含まれるはずである。メタデータ同化および入力ツール161は、コンテンツ・プロバイダのデータベース160またはコンテンツ・プロバイダによって所定のフォーマットで供給されるデータからメタデータ(音楽の例の場合、CDタイトル、アーティスト名、曲の題名、CDアートワークその他などのコンテンツ113の情報)を抽出し、電子配布のためにパッケージ化するのに使用される。メタデータ同化および入力ツール161は、コンテンツ113の使用条件を入力するのにも使用される。使用条件のデータには、コピー制限規則、卸値、および必要とみなされるすべてのビジネス・ルールを含めることができる。ウォーターマーキング・ツールが、コンテンツ113内の、コンテンツ所有者、処理日付、および他の関連データを識別するデータを隠すのに使用される。コンテンツ113がオーディオである実施形態では、オーディオ・プリプロセッサ・ツールを使用して、最適の圧縮品質のために動的特性を調整するかコンテンツ113または他のオーディオを等化し、所望の圧縮レベルまでコンテンツ113を圧縮し、コンテンツ113を暗号化する。これらは、ディジタル・コンテンツ圧縮／符号化方法、暗号化方法、およびフォーマッティング方法の技術的進歩に従うように適合することができ、これによって、コンテンツ・プロバイダ101が、将来市場に現れる最適のツールを利用することができるようになる。

【0034】暗号化されたコンテンツ113、ディジタル・コンテンツに関連するデータまたはメタデータ、および暗号化された鍵が、SCパッカー・ツールによってSC(下で説明する)にパックされ、電子配布のためにコンテンツ・ホスティング・サイトまたは販売促進ウェブ・サイトに格納される。コンテンツ・ホスティング・サイトは、コンテンツ・プロバイダ101または、電子ディジタル・コンテンツ商店103および仲介市場パートナー(図示せず)施設を含む複数の位置に存在することができる。コンテンツ113と鍵(下で説明する)の両方が、暗号化され、SCにパックされるので、電子ディジタル・コンテンツ商店103または他のホスティング代理人は、クリアリングハウスからの許可およびコンテンツ・プロバイダ101への通知なしで、解読されたコンテンツ113に直接アクセスすることはできない。

【0035】2. 電子ディジタル・コンテンツ商店103電子ディジタル・コンテンツ商店103は、コンテンツ113のテーマ・プログラミングまたはコンテンツ113の電子マーチャンダイジングなどの広範囲のサービスまたはアプリケーションを介してコンテンツ113を市場で売る実体である。電子ディジタル・コンテンツ商店103は、そのサービスの設計、開発、ビジネス運営、決定、マーチャンダイジング、マーケティング、および販売を管理する。オンラインの電子ディジタル・コンテンツ商店103の例が、ソフトウェアの電子ダウンロードを提供するウェブ・サイトである。

【0036】そのサービスの中で、電子ディジタル・コンテンツ商店103は、セキュア・ディジタル・コンテンツ電子配布システム100のいくつかの機能を実施する。電子ディジタル・コンテンツ商店103は、コンテンツ・プロバイダ101から情報を集め、コンテンツおよびメタデータを追加SCにパックし、これらのSCをサービスまたはアプリケーションの一部として消費者または企業に配布する。電子ディジタル・コンテンツ商店103は、メタデータ抽出、2次使用条件、SCパッケージ化、および電子コンテンツ・トランザクションの追跡を支援する、セキュア・ディジタル・コンテンツ電子配布システム100によって提供されるツールを使用する。2次使用条件データには、コンテンツ113の購入価格、ペイパーリスン(pay-per-listen)価格、コピー許可およびターゲット装置タイプ、または期限付き使用可能性制限などの小売りビジネス・オファーを含めることができる。

【0037】電子ディジタル・コンテンツ商店103は、エンドユーザからの電子的なコンテンツ113の有効な要求を完了した後に、クリアリングハウス105が顧客にコンテンツ113の解読キーを公開することを許可する責任を負う。電子ディジタル・コンテンツ商店は、コンテンツ113を含むSCのダウンロードも許可する。電子ディジタル・コンテンツ商店は、そのローカル・サイトでディジタル・コンテンツを含むSCをホストするか、別のコンテンツ・ホスティング・サイトのホスティング施設および配布施設を使用するか、その両方を行うかを選択することができる。

【0038】電子ディジタル・コンテンツ商店は、セキュア・ディジタル・コンテンツ電子配布システム100を使用するエンドユーザが持つ可能性がある質問または問題に関するカスタマ・サービスを提供することができ、また、電子ディジタル・コンテンツ商店103は、カスタマ・サービス・サポートについてクリアリングハウス105と契約することができる。

【0039】3. 仲介市場パートナー(図示せず)

代替実施形態では、セキュア・ディジタル・コンテンツ電子配布システム100を使用して、仲介市場パートナーと呼ばれる他の会社にコンテンツ113を保護された形で供給することができる。これらのパートナーには、テレビ局またはビデオ・クラブ、ラジオ局またはレコード・クラブなどの非電子サービスを提供する、コンテンツ113を供給するディジタル・コンテンツ関連会社を含めることができる。これらのパートナーには、録音スタジオ、レプリケータ(replicator)、およびプロデューサなどの、サウンド・レコーディングの製作またはマーケティングの一部として素材を扱う他の信頼される当事者も含めることができる。これらの仲介市場パートナーは、コンテンツ113を解読するために、クリアリングハウス105からの許可を必要とする。

【0040】4. クリアリングハウス105クリアリングハウス105は、ライセンス交付許可と、SC内で暗号化されたコンテンツ113の販売または許可される使用に関係するすべてのトランザクションに関する記録保持を提供する。クリアリングハウス105は、仲介者またはエンドユーザからコンテンツ113の解読キーの要求を受け取った時に、要求内の情報の保全性および認証性を検証し、その要求が電子ディジタル・コンテンツ商店またはコンテンツ・プロバイダ101によって許可されたことを検証し、要求された使用が、コンテンツ・プロバイダ101によって定義されるコンテンツの使用条件に従うことを検証する。これらの検証が満足された後に、クリ

アリングハウス105は、コンテンツ113の解読キーを、ライセンスSCにパックして要求元のエンドユーザに送る。鍵は、許可されたユーザだけが取り出せる形で暗号化される。エンドユーザの要求が検証可能でないか、完全でないか、許可されない場合には、クリアリングハウス105は、解読キーの要求を拒絶する。

【0041】クリアリングハウス105は、すべてのトランザクションの記録を保持し、電子ディジタル・コンテンツ商店103およびコンテンツ・プロバイダ101などの責任を持つ当事者に、即座に、周期的に、または制限された形で、その記録を報告することができる。この報告は、コンテンツ・プロバイダ101が、コンテンツ113の販売について知らされる手段であり、電子ディジタル・コンテンツ商店103が、その顧客への電子配布の監査証跡を得ることのできる手段である。クリアリングハウス105は、SC内の情報が損なわれたかコンテンツの使用条件に従わないことを検出した場合にも、コンテンツ・プロバイダ101または電子ディジタル・コンテンツ商店103もしくはその両方に通知することができる。クリアリングハウス105のデータベースのトランザクション記録機能およびリポジトリ機能は、データ・マイニングおよび報告生成用に構成されている。

【0042】もう1つの実施形態では、クリアリングハウス105は、払い戻し、伝送障害、購入上の論争などの、カスタマ・サポートおよびトランザクションに関する例外処理を提供することができる。クリアリングハウス105は、独立の実体として運営され、権利管理および測定の信頼される管理者となることができる。クリアリングハウス105は、必要に応じて請求および清算を提供する。電子クリアリングハウスの例には、Secure-Bank.comおよびVisa/Mastercard社のSET（Secure Electronic Transaction）が含まれる。一実施形態では、クリアリングハウス105は、エンドユーザ装置109からアクセス可能なウェブ・サイトである。もう1つの実施形態では、クリアリングハウス105は、電子ディジタル・コンテンツ商店103の一部である。

【0043】5. エンドユーザ装置109エンドユーザ装置109は、セキュア・ディジタル・コンテンツ電子配布システム100仕様に従うプレイヤ・アプリケーション195（後で説明する）を含むプレイヤ装置とすることができる。これらの装置には、PCS、セット・トップ・ボックス（IRD）、およびインターネット機器が含まれる。プレイヤ・アプリケーション195は、ソフトウェアまたは消費者エレクトロニクス・ハードウェアもしくはその両方で実施することができる。再生機能、記録機能、およびライブラリ管理機能を実行するほかに、プレイヤ・アプリケーション195は、エンドユーザ装置109での権利管理を可能にするためのSC処理を実行する。エンドユーザ装置109は、ディジタル・コンテンツを含むSCのダウンロードおよび格納を管理し、クリアリングハウス105に暗号化されたディジタル・コンテンツ鍵を要求し、その受取を管理し、ディジタル・コンテンツがコピーまたは再生されるたびに透かしを処理し、ディジタル・コンテンツの使用条件に従って、作られるコピー（またはコピーの削除）の数を管理し、許可される場合に、外部媒体またはポータブル消費者装置へのコピーを実行する。ポータブル消費者装置は、透かしに埋め込まれたコンテンツの使用条件を処理するために、プレイヤ・アプリケーション195の機能のサブセットを実行することができる。用語エンドユーザおよびプレイヤ・アプリケーション195は、本明細書全体を通じて、エンドユーザ装置109の使用またはエンドユーザ装置109上での実行を介することを意味するために使用される。

【0044】6. 伝送インフラストラクチャ107セキュア・ディジタル・コンテンツ電子配布システム100は、電子ディジタル・コンテンツ商店103とエンドユーザ装置109を接続する伝送ネットワークからの独立である。セキュア・ディジタル・コンテンツ電子配布システム100は、インターネットなどの2地点間モデルと、ディジタル放送テレビジョンなどのブロードキャスト配布モデルの両方をサポートする。

【0045】さまざまな伝送インフラストラクチャ107でのコンテンツ113のトランザクションの獲得、パッケージ化、および追跡に同一のツールおよびアプリケーションが使用されるが、そのプレゼンテーションおよび、サービスが顧客に配送される方法は、選択されたインフラストラクチャおよび配布モデルに依存して変化する場合がある。転送されるコンテンツ113の品質も、変化する場合がある。というのは、高帯域幅インフラストラクチャが、低帯域幅インフラストラクチャより許容可能な応答時間で高品質のディジタル・コンテンツを配送できるからである。2地点間配布モデル用に設計されたサービス・アプリケーションを、ブロードキャスト配布モデルもサポートするように適合させることができる。

【0046】C. システムの使用セキュア・ディジタル・コンテンツ電子配布システム100を用いると、消費者または企業のいずれかであるエンドユーザ装置109へのコンテンツ113の高品質電子コピーの安全な配布が可能になり、コンテンツ113の使用の調整および追跡が可能になる。

【0047】セキュア・ディジタル・コンテンツ電子配布システム100は、新しい配布チャネルと既存の配布チャネルの両方を使用して、さまざまな消費者サービスおよび企業対企業サービスで展開することができる。各特定のサービスでは、セキュア・ディジタル・コンテンツ電子配布システム100の権利管理機能を介して実施することができる異なる財政モデルを使用することができる。卸売または小売り購入、ペイパーリスン使用料、購買契約サービス、コピー制限／コピー無制限、または再配布などのモデルを、クリアリングハウス105の権利管理およびエンドユーザのプレイヤ・アプリケーション195のコピー・プロテクション機能を介して実施することができる。

【0048】セキュア・ディジタル・コンテンツ電子配布システム100を用いると、電子ディジタル・コンテンツ商店103および仲介市場パートナーが、コンテンツ113を販売するサービスを作成する際に非常に高い柔軟性を与えられる。それと同時に、コンテンツ・プロバイダ101に、彼らのディジタル資産が保護され、測定され、その結果、彼らがコンテンツ113のライセンス交付に対する適当な報酬を受け取ることができることの、あるレベルの保証が与えられる。

【0049】II. 暗号の概念とセキュア・ディジタル・コンテンツ電子配布システムへの適用セキュア・ディジタル・コンテンツ電子配布システム100のライセンス制御は、暗号の使用に基づく。この節では、本発明の基本的な暗号技術を紹介する。公開鍵暗号、対称鍵暗号、ディジタル署名、ディジタル透かし、およびディジタル証明書の使用は、既知である。

【0050】A. 対称アルゴリズムセキュア・ディジタル・コンテンツ電子配布システム100では、コンテンツ・プロバイダ101が、対称アルゴリズムを使用してコンテンツを暗号化する。これが対称アルゴリズムと呼ばれるのは、データの暗号化と解読に同一の鍵が使用されるからである。データを送る側とメッセージを受け取る側が、その鍵を共用しなければならない。この共用鍵を、本明細書では対称鍵と呼ぶ。セキュア・ディジタル・コンテンツ電子配布システム100のアーキテクチャは、特定の実施態様について選択される特定の対称アルゴリズムからの独立である。

【0051】一般的な対称アルゴリズムが、DES、RC2、およびRC4である。DESとRC2の両方が、ブロック暗号である。ブロック暗号では、1時にデータ・ビットのブロックを使用してデータを暗号化する。DESは、米国政府公認の暗号化標準規格であり、64ビットのブロック・サイズを有し、56ビットの鍵を使用する。単純なDESを用いて達成されるセキュリティを高めるために、一般にトリプルDESが使用される。RSA Data Securityが、RC2を設計した。RC2は、可変鍵サイズ暗号を使用し、64ビットのブロック・サイズを有する。やはりRSA Data Securityが設計したRC4は、可変鍵サイズ・ストリーム暗号である。ストリーム暗号は、1時に1データ・ビットを操作する。RSA Data Securityは、RC4の場合に、出力1バイトごとに8ないし16個の機械動作が必要であると主張している。

【0052】IBMは、SEALと呼ばれる高速アルゴリズムを設計した。SEALは、可変長鍵を使用し、32ビット・プロセッサ用に最適化された、ストリーム・アルゴリズムである。SEALは、データ・バイトごとに約5個の基本機械語命令を必要とする。50MHzの486ベースのコンピュータは、使用される160ビットの鍵がすでに前処理されて内部テーブルに格納されている場合に、SEALコードを7. 2メガバイト／秒で実行する。

【0053】Microsoftは、そのOverview of CryptoAPI文書で、暗号化性能ベンチマークの結果を報告した。これらの結果は、MicrosoftのCryptoAPIを使用するアプリケーションによって、120MHzのPentium（登録商標）ベースでWindows NT（登録商

標）4．0が動作するコンピュータで得られた。
【0054】
【表1】

暗号	鍵サイズ	鍵セットアップ時間	暗号化速度
DES	56	460	1,138,519
RC2	40	40	286,888
RC4	40	151	2,377,723

【0055】B．公開鍵アルゴリズムセキュア・ディジタル・コンテンツ電子配布システム100では、対称鍵および他の小さいデータが、公開鍵を使用して暗号化される。公開鍵アルゴリズムでは、2つの鍵を使用する。2つの鍵は、数学的に関係しており、その結果、一方の鍵を用いて暗号化されたデータは、他方の鍵を用いなければ解読できない。鍵の所有者は、一方の鍵（秘密鍵）を秘密に保ち、第2の鍵（公開鍵）を一般に配布する。
【0056】公開鍵アルゴリズムを使用して機密メッセージの伝送を保護するためには、受取り側の公開鍵を使用してメッセージを暗号化しなければならない。関連する秘密鍵を有する受取り側だけが、そのメッセージを解読することができる。公開鍵アルゴリズムは、ディジタル署名の生成にも使用される。その目的には、秘密鍵が使用される。次の節で、ディジタル署名に関する情報を示す。
【0057】最も一般的に使用されている公開鍵アルゴリズムは、RSA公開鍵暗号である。RSAは、当産業で事実上の公開鍵標準になった。暗号化およびディジタル署名のために同様に良好に機能する他のアルゴリズムが、ElGamalおよびRabinである。RSAは、可変鍵長暗号である。
【0058】対称鍵アルゴリズムは、公開鍵アルゴリズムよりはるかに高速である。ソフトウェアでは、DESは、一般にRSAより少なくとも100倍高速である。このため、RSAは、大量のデータの暗号化には使用されない。RSA Data Securityは、90MHzのPentium計算機上で、RSA Data SecurityのツールキットBSAFE 3．0が、512ビットの法を用いて21．6キロビット／秒、1024ビットの法を用いて7．4キロビット／秒の秘密鍵操作（秘密鍵を使用する暗号化または解読）のスループットを有すると報告した。
【0059】C．ディジタル署名セキュア・ディジタル・コンテンツ電子配布システム100では、SCの発行者が、それにディジタル署名することによってSCの保全性を保護する。一般に、メッセージのディジタル署名を作成するためには、メッセージ所有者が、まず、メッセージ・ダイジェスト（下で定義する）を計算し、その後、所有者の秘密鍵を使用してメッセージ・ダイジェストを暗号化する。メッセージは、その署名と共に配布される。メッセージの受取り側は、まずメッセージ所有者の公開鍵を使用して署名を解読して、メッセージ・ダイジェストを回復することによって、ディジタル署名を検証することができる。次に、受取り側は、受け取ったメッセージのダイジェストを計算し、回復されたダイジェストと比較する。メッセージが配布中に変更されていない場合には、計算されたダイジェストと回復されたダイジェストが等しくならなければならない。
【0060】セキュア・ディジタル・コンテンツ電子配布システム100では、SCに複数のデータ部分が含まれるので、ダイジェストが、部分ごとに計算され、合計ダイジェストが、連結された部分ダイジェストについて計算される。合計ダイジェストは、SCの発行者の秘密鍵を使用して暗号化される。暗号化された合計ダイジェストが、SCの発行者のディジタル署名になる。部分ダイジェストおよびディジタル署名は、SCの本体に含まれる。SCの受取り側は、受け取ったディジタル署名および部分ダイジェストによって、SCとその諸部分の保全性を検証することができる。
【0061】一方向ハッシュ・アルゴリズムが、メッセージ・ダイジェストの計算に使用される。ハッシュ・アルゴリズムは、可変長入力メッセージをとり、固定長文字列すなわちメッセージ・ダイジェストに変換する。一方向ハッシュ・アルゴリズムは、一方向だけに動作する。すなわち、入力メッセージからダイジェストを計算することは簡単であるが、ダイジェストから入力メッセージを生成することは非常に困難（計算的に実行不可能）である。一方向ハッシュ関数の特性のゆえに、メッセージ・ダイジェストを、メッセージの指紋と考えることができる。
【0062】より一般的な一方向ハッシュ関数が、RSA Data SecurityのMD5および、NIST（米国連邦情報・技術局）によって設計されたSHAである。
【0063】D．ディジタル証明書ディジタル証明書は、ディジタル署名されたメッセージを送った人物または実体の身元を認証または検証するのに使用される。証明書は、公開鍵を人物または実体に結び付ける証明機関によって発行されるディジタル文書である。証明書には、公開鍵、人物または実体の名前、満了期日、証明機関の名前、および他の情報が含まれる。証明書には、証明機関のディジタル署名も含まれる。
【0064】実体（または人物）が、その秘密鍵を用いて署名され、ディジタル証明書を添付されたメッセージを送る時には、そのメッセージの受取り側は、証明書の実体の名前を使用して、メッセージを受け入れるか否かを決定する。
【0065】セキュア・ディジタル・コンテンツ電子配布システム100では、エンドユーザ装置109によって発行されるものを除くすべてのSCに、SCの作成者の証明書が含まれる。多数のエンドユーザ装置が、証明書を取得することさえしないか、真正でない証明機関によって発行された証明書を有するので、エンドユーザ装置109が、そのSCに証明書を含める必要はない。セキュア・ディジタル・コンテンツ電子配布システム100では、クリアリングハウス105は、電子ディジタル・コンテンツ商店103に証明書を発行するというオプションを有する。これによって、エンドユーザ装置109は、電子ディジタル・コンテンツ商店103がセキュア・ディジタル・コンテンツ電子配布システム100によって認証されたことを独立に検証できるようになる。
【0066】E．SCグラフィカル表現の案内この文書では、暗号化された部分、暗号化されない部分、暗号鍵、および証明書を示す図面を使用して、SCをグラフィカルに表現する。ここで図5を参照すると、図5はSC200の例の図である。以下の記号が、SCの図で使用されている。鍵201は、公開鍵または秘密鍵である。鍵の歯、たとえばクリアリングハウスを表すCLRNGHは、鍵の所有者を示す。ハンドルの中のPBは、それが公開鍵であることを示し、したがって、鍵201は、クリアリングハウスの公開鍵である。ハンドルの中のPVは、それが秘密鍵であることを示す。ひし形は、エンドユーザ・ディジタル署名202である。頭文字は、その署名を作成するのに使用された秘密鍵を示し、したがって、EUは、下の表からエンドユーザのディジタル署名である。対称鍵203は、コンテンツの暗号化に使用される。暗号化された対称鍵オブジェクト204には、CLRNGHのPBを用いて暗号化された対称鍵203が含まれる。この長方形の上辺の鍵は、オブジェクトの暗号化に使用された鍵である。長方形の内部の記号またはテキストは、暗号化されたオブジェクト（この例では対称鍵）を表す。もう1つの暗号化されたオブジェクト、この例ではトランザクションID暗号化オブジェクト205が示されている。さらに、下で説明するコンテンツ・ライセンス交付管理のための使用条件206がある。SC200には、使用条件206、トランザクションID暗号化オブジェクト205、アプリケーションID暗号化オブジェクト207、および暗号化された対称鍵オブジェクト204が含まれ、これらのすべてが、エンドユーザ・ディジタル署名202によって署名される。
【0067】次の表に、SCの署名者を識別する頭文字を示す。
【表2】

頭文字	コンポーネント
CP	コンテンツ・プロバイダ101
MS	電子ディジタル・コンテンツ店舗103
HS	コンテンツ・ホスティング・サイト111
EU	エンドユーザ装置109
CH	クリアリングハウス105
CA	証明機関（図示せず）

【0068】F. セキュア・コンテナ暗号化の例下の表およびダイアグラムに、SCからの情報の作成および回復に使用される暗号化および解読の処理の概要を示す。この処理の概要で作成され解読されるSCは、一般的なSCである。これは、セキュア・ディジタル・コンテンツ電子配布システム100の権利管理に使用される特定のSCタイプを表すものではない。この処理は、暗号化処理について図6に記載されたステップからなる。
【0069】図6の暗号化処理の処理フローステップ 処理301 送信元が、ランダムな対称鍵を生成し、それを使用してコンテンツを暗号化する。
302 送信元が、暗号化されたコンテンツをハッシュ・アルゴリズムにかけて、コンテンツ・ダイジェストを作る。
303 送信元が、受取り側の公開鍵を使用して対称鍵を暗号化する。PBRECPNTは、受取り側の公開鍵を指す。
304 送信元が、ステップ2で使用したものと同一のハッシュ・アルゴリズムに、暗号化された対称鍵をかけて、対称鍵ダイジェストを作る。
305 送信元が、ステップ2で使用したものと同一のハッシュ・アルゴリズムに、コンテンツ・ダイジェストおよび対称鍵ダイジェストの連結をかけて、SCダイジェストを作る。
306 送信元が、送信元の秘密鍵を用いてSCダイジェストを暗号化して、SCのディジタル署名を作る。PV SENDERは、送信元の秘密鍵を指す。
307B 送信元が、暗号化されたコンテンツ、暗号化された対称鍵、コンテンツ・ダイジェスト、対称鍵ダイジェスト、送信元の証明書、およびSC署名を含むSCファイルを作成する。
307A 送信元は、セキュア通信を開始する前に、証明機関から証明書を入手していなければならない。証明機関は、証明書に、送信元の公開鍵および送信元の名前を含め、それに署名する。PV CAUTHRは、証明機関の秘密鍵を指す。送信元が、SCを受取り側に送信する。
【0070】図7の解読処理の処理フローステップ 処理408 受取り側が、SCを受信し、その諸部分を分離する。
409 受取り側が、証明機関の公開鍵を用いて送信元の証明書のディジタル署名を解読することによって、送信元の証明書のディジタル署名を検証する。証明書のディジタル署名が有効である場合には、受取り側は、証明書から送信元の公開鍵を獲得する。
410 受取り側が、送信元の公開鍵を使用してSCディジタル署名を解読する。これによってSCダイジェストが回復される。PB SENDERは、送信元の公開鍵を指す。
411 受取り側が、受信したコンテンツ・ダイジェストおよび暗号化された鍵ダイジェストの連結を、送信元がSCダイジェストの計算に使用したものと同一のハッシュ・アルゴリズムにかける。
412 受取り側が、計算されたSCダイジェストを、送信元のディジタル署名から回復されたSCダイジェストと比較する。これらが同一である場合には、受取り側は、受信したダイジェストが変更されていないことを確認し、解読処理を継続する。これらが同一でない場合には、受取り側は、SCを破棄し、送信元に通知する。
413 受取り側が、暗号化された対称鍵を、ステップ411で対称鍵ダイジェストの計算に使用したものと同一のハッシュ・アルゴリズムにかける。
414 受取り側が、計算された対称鍵ダイジェストを、SC内で受け取った対称鍵ダイジェストと比較する。これが同一である場合には、受取り側は、暗号化された対称鍵が変更されていないことを知る。受取り側は、解読処理を継続する。有効でない場合には、受取り側は、SCを破棄し、送信元に通知する。
415 受取り側が、暗号化されたコンテンツを、ステップ411でコンテンツ・ダイジェストの計算に使用したものと同一のハッシュ・アルゴリズムにかける。
416 受取り側が、計算されたコンテンツ・ダイジェストを、SC内で受け取ったコンテンツ・ダイジェストと比較する。それが同一である場合には、受取り側は、暗号化されたコンテンツが変更されていないことを知る。受取り側は、解読処理を継続する。有効でない場合には、受取り側は、SCを破棄し、送信元に通知する。
417 受取り側は、受取り側の秘密鍵を使用して、暗号化された対称鍵を解読する。これによって、対称鍵が回復される。PV RECPNTは、受取り側の秘密鍵を指す。
418 受取り側が、対称鍵を使用して、暗号化されたコンテンツを解読する。これによって、コンテンツが回復される。
【0071】III. セキュア・ディジタル・コンテンツ電子配布システムのフローセキュア・ディジタル・コンテンツ電子配布システム100は、システムの異なる参加者によって使用される複数のコンポーネントからなる。この参加者には、コンテンツ・プロバイダ101、電子ディジタル・コンテンツ商店103、エンドユーザ装置109を介するエンドユーザ、およびクリアリングハウス105が含まれる。高水準システム・フローを、セキュア・ディジタル・コンテンツ電子配布システム100の概要として使用する。下に輪郭を示すこのフローでは、セキュア・ディジタル・コンテンツ電子配布システム100を流れるコンテンツを追跡する。さらに、コンテンツ113の購入、ロック解除、および使用のためのトランザクションを行うために参加者が使用するステップの輪郭を示す。このシステム・フローでの仮定の一部には、下記が含まれる。
・これは、ディジタル・コンテンツ・サービス（PCへの2地点間インターフェース）のシステム・フローである。
・コンテンツ・プロバイダ101は、PCM非圧縮フォーマットでオーディオ・ディジタル・コンテンツをサブミットする（音楽オーディオの例として）。
・コンテンツ・プロバイダ101は、ODBC準拠データベースにメタデータを有するか、コンテンツ・プロバイダ101は、コンテンツ情報処理サブシステムに直接にデータを入力するか、所定のASCIIファイル・フォーマットでデータを供給する。
・会計清算は、電子ディジタル・コンテンツ商店によって行われる。
・コンテンツ113は、単一のコンテンツ・ホスティング・サイト111でホストされる。
【0072】当業者は、ディジタル・コンテンツの正確な性質、たとえば、音楽、ビデオ、およびプログラムと電子配布システム・ブロードキャストに対応するために、これらの仮定を変更できることを理解されたい。
【0073】次の処理フローは、図1ないし4に示されている。

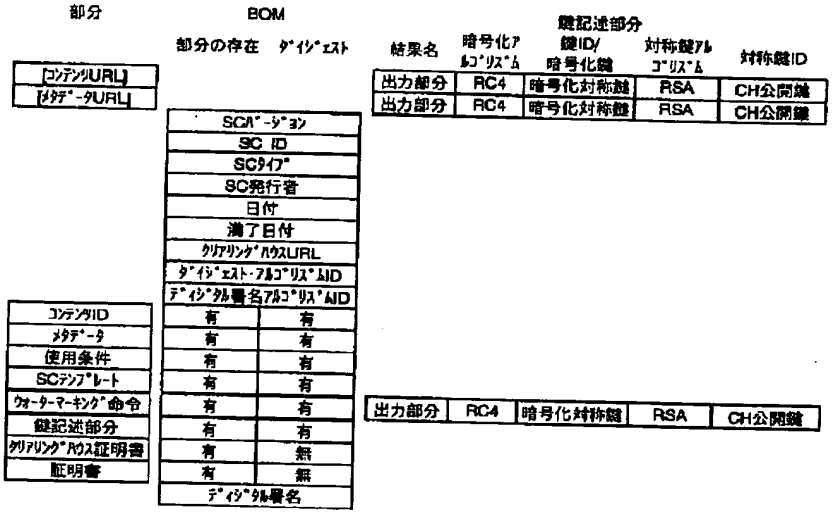
ステップ 処理121 非圧縮PCMオーディオ・ファイルが、コンテンツ・プロバイダ101によってコンテンツ113として供給される。そのファイル名が、コンテンツ・プロバイダ101のコンテンツ113の一意の識別子と共にワーク・フロー・マネージャ154に入力される。
122 メタデータが、コンテンツ・プロバイダ101のコンテンツ113の一意の識別子およびデータベース・マッピング・テンプレートによって供給される情報を使用して、コンテンツ情報処理サブシステムによってコンテンツ・プロバイダのデータベース160に収集される。
123 ワーク・フロー・マネージャ154を使用して、コンテンツ・プロバイダ101での獲得および準備処理を通るようにコンテンツ・フローを向ける。ワーク・フロー・マネージャ154は、任意の時点でシステム内のコンテンツの部分の状況を追跡するのに使用することもできる。
124 コンテンツ113の使用条件が、コンテンツ情報処理サブシステムに入力されるが、これは、手動でまたは自動的にのいずれかで行うことができる。このデータには、コピー制限規則と、必要とみなされる他のビジネス・ルールが含まれる。メタデータ入力のすべてを、データのオーディオ処理と並列に行うことができる。
125 ウォーターマーキング・ツールを使用して、コンテンツ・プロバイダ101がコンテンツの識別に必要とみなすデータを、コンテンツ113内に隠す。これには、いつそれが収集されたか、それがどこから来たか(このコンテンツ・プロバイダ101)、またはコンテンツ・プロバイダ101によって指定される他の情報を含めることができる。
・コンテンツ処理ツール125が、サポートされる異なる圧縮レベルに必要な、コンテンツ113の等化、動的特性調整および再サンプリングを実行する。
・コンテンツ処理ツール125を使用して、コンテンツ113を所望の圧縮レベルまで圧縮する。その後、コンテンツ113を再生して、圧縮によってコンテンツ113に必要な品質レベルが作られたことを検証することができる。必要であれば、等化、動的特性調整、圧縮、および再生品質検査を、望む回数だけ実行することができる。
・コンテンツ113およびそのメタデータのサブセットを、SCパッカーによって対称鍵を用いて暗号化する。その後、このツールは、クリアリングハウス105の公開鍵を使用してその鍵を暗号化して、暗号化された対称鍵を作る。この鍵は、それを解読できる実体がクリアリングハウス105だけなので、コンテンツ113のセキュリティを危険にさらすことなくどこにでも送信することができる。
126 暗号化された対称鍵、メタデータ、およびコンテンツ113に関する他の情報を、SCパッカー・ツール152がメタデータSCにパックする。
127 暗号化されたコンテンツ113およびメタデータを、コンテンツSCにパックする。この時点で、コンテンツ113およびメタデータの処理が完了する。
128 メタデータSCを、コンテンツ分配ツール(図示せず)を使用してコンテンツ販売促進ウェブ・サイト156に送信する。
129 コンテンツ分配ツールが、コンテンツSCをコンテンツ・ホスティング・サイト111に送信する。コンテンツ・ホスティング・サイトは、コンテンツ・プロバイダ101、クリアリングハウス105、またはコンテンツ・ホスティング専用の特殊な場所に存在することができる。このサイトのURLは、メタデータSCに追加されるメタデータの一部である。
130 コンテンツ販売促進ウェブ・サイト156が、セキュア・ディジタル・コンテンツ電子配布システム100に追加された新しいコンテンツ113について電子ディジタル・コンテンツ商店103に通知する。
131 コンテンツ獲得ツールを使用して、電子ディジタル・コンテンツ商店103が、それが販売を望むコンテンツ113に対応するメタデータSCをダウンロードする。
132 電子ディジタル・コンテンツ商店103は、コンテンツ獲得ツールを使用して、そのウェブ・サイトでのコンテンツ113の販売促進に使用したいデータをメタデータSCから引き出す。このメタデータの諸部分へのアクセスは、望むならば保護し、料金を請求することができる。
133 電子ディジタル・コンテンツ商店103に固有の、コンテンツ113の使用条件を、コンテンツ獲得ツールを使用して入力する。この使用条件には、コンテンツ113の異なる圧縮レベルの、小売り価格およびコピー/再生制限が含まれる。
134 電子ディジタル・コンテンツ商店103に固有の使用条件およびオリジナルのメタデータSCを、SCパッカー・ツールによってオファーSCにパックする。
135 電子ディジタル・コンテンツ商店103のウェブ・サイトを更新した後に、コンテンツ113が、そのウェブを訪れるエンドユーザに入手可能になる。
136 エンドユーザは、購入したいコンテンツ113を見つけた時に、音楽アイコンなどのコンテンツ・アイコンをクリックし、その項目が、電子ディジタル・コンテンツ商店103が維持するエンドユーザのショッピング・カートに追加される。エンドユーザは、ショッピングを完了した時に、処理のために電子ディジタル・コンテンツ商店103に購入要求をサブミットする。
137 電子ディジタル・コンテンツ商店103は、クレジット・カード清算組織と対話して、現在業務を行っているのと同じ形で資金を確保する。
138 電子ディジタル・コンテンツ商店103は、クレジット・カード清算組織からクレジット・カード認証番号を受信した後に、これをデータベースに格納し、SCパッカー・ツールを呼び出して、トランザクションSCを作成する。このトランザクションSCには、エンドユーザが購入したコンテンツ113に関するオファーSCのすべて、電子ディジタル・コンテンツ商店103までさかのぼって追跡することができるトランザクションID、エンドユーザを識別する情報、購入した曲の圧縮レベル、使用条件および価格リストが含まれる。
139 このトランザクションSCを、エンドユーザ装置109に送信する。
140 トランザクションSCが、エンドユーザ装置109に到達した時に、プレイヤ・アプリケーション195が開始され、プレイヤ・アプリケーション195が、トランザクションSCをオープンし、エンドユーザの購入を確認する。プレイヤ・アプリケーション195は、個々のオファーSCをオープンし、代替実施形態では、ダウンロード時間の推定値をユーザに知らせることができる。その後、プレイヤ・アプリケーション195は、コンテンツ113をいつダウンロードするかを指定するようにユーザに求める。
141 エンドユーザがダウンロードを要求した時刻に基づいて、プレイヤ・アプリケーション195が覚醒し、とりわけコンテンツ113の暗号化された対称鍵、トランザクションID、およびエンドユーザ情報を含む注文SCを作成することによって、ダウンロード処理の開始を開始する。
142 この注文SCを、処理のためにクリアリングハウス105に送信する。
143 クリアリングハウス105が、注文SCを受信し、それをオープンし、データのすべてが変更されていないことを検証する。クリアリングハウス105は、エンドユーザが購入した使用条件を検証する。この使用条件は、コンテンツ・プロバイダ101によって指定された使用条件に従わなければならない。この情報は、データベースにログ記録される。
144 すべての検査が完了した後に、クリアリングハウス105の秘密鍵を使用して、暗号化された対称鍵を解読する。次に、この対称鍵を、エンドユーザの公開鍵を使用して暗号化する。この新たに暗号化された対称鍵を、SCパッカーによってライセンスSCにパッケージ化する。
145 ライセンスSCを、エンドユーザに送信する。
146 ライセンスSCをエンドユーザ装置109が受信した時に、そのライセンスSCは、コンテンツSCがダウンロードされるまでメモリに格納される。
147 エンドユーザ装置109は、コンテンツ・ホスティング・サイト施設111に、対応するライセンスSCを送信して、購入したコンテン

ツ113を要求する。
148 コンテンツ113が、エンドユーザ装置109に送信される。受信時に、コンテンツ113は、エンドユーザ装置109によって、対称鍵を使用して暗号解読される。
【0074】IV. 権利管理アーキテクチャ・モデルA. アーキテクチャ層の機能図8は、セキュア・ディジタル・コンテンツ電子配布システム100の権利管理アーキテクチャのブロック図である。アーキテクチャ的には、4つの層すなわち、ライセンス制御層501、コンテンツ識別層503、コンテンツ使用制御層505、およびコンテンツ・フォーマッティング層507が、セキュア・ディジタル・コンテンツ電子配布システム100を表す。各層の総合的な機能目的と、各層の個々の主要機能を、この節で説明する。層のそれぞれの機能は、他の層の機能からかなり独立している。広い制限の中で、ある層の機能を、他の層の機能に影響せずに類似する機能と置換することができる。明らかに、ある層の出力は、隣接する層が受け入れることのできるフォーマットおよびセマンティクスを満足することが必要である。
【0075】ライセンス制御層501は、以下を保証する。
・ディジタル・コンテンツが、配布中に不法な傍受および変更から保護される。
・コンテンツ113が、合法的なコンテンツ所有者から発し、ライセンスを交付されたディストリビュータ、たとえば電子ディジタル・コンテンツ商店103によって配布される。
・ディジタル・コンテンツ購入者が、正しくライセンスを交付されたアプリケーションを有する。
・コンテンツ113のコピーが購入者またはエンドユーザに使用可能にされる前に、ディストリビュータが、購入者から支払を受ける。
・報告のためにトランザクションの記録が保存される。
【0076】コンテンツ識別層503は、著作権およびコンテンツ購入者の識別の検証を可能にする。コンテンツの著作権情報およびコンテンツ購入者の識別によって、コンテンツ113の、許可されたコピーまたは許可されないコピーの出所追跡が可能になる。したがって、コンテンツ識別層503は、海賊行為と戦う手段を提供する。
【0077】コンテンツ使用制御層505は、コンテンツ113のコピーが、商店使用条件519に従って購入者の装置で使用されることを保証する。商店使用条件519では、コンテンツ113について許可される再生回数およびローカル・コピーの数と、コンテンツ113を外部ポータブル装置に記録することができるか否かを指定することができる。コンテンツ使用制御層505の諸機能は、コンテンツのコピー／再生使用量を追跡し、コピー／再生状況を更新する。
【0078】コンテンツ・フォーマッティング層507は、コンテンツ所有者の施設でのコンテンツ113のネイティブ表現から、セキュア・ディジタル・コンテンツ電子配布システム100のサービス機能および配布手段との一貫性を有する形式へのコンテンツ113のフォーマット変換を可能にする。変換処理には、圧縮符号化とそれに関連する前処理、たとえば周波数等化および振幅動的調整を含めることができる。オーディオのコンテンツ113の場合、購入者の側でも、受信したコンテンツ113を処理して、再生またはポータブル装置への転送に適したフォーマットを達成する必要がある。
【0079】B. 機能の区分とフロー権利管理アーキテクチャ・モデルが、図8に示されており、これは、セキュア・ディジタル・コンテンツ電子配布システム100を構成するオペレーティング・コンポーネントへのアーキテクチャ層のマッピングおよび各層の主要な機能を示す図である。
【0080】1. コンテンツ・フォーマッティング層507コンテンツ・フォーマッティング層507に関連する一般的な機能は、コンテンツ・プロバイダ101のコンテンツ前処理502およびコンテンツ圧縮511と、エンドユーザ装置109のコンテンツ・スクランブル解除513およびコンテンツ圧縮解除515である。前処理の必要および具体的な機能の例は、上で述べた。コンテンツ圧縮511は、コンテンツ113のファイル・サイズと伝送時間を減らすのに使用される。コンテンツ113および伝送媒体の種類に適当な任意の圧縮アルゴリズムを、セキュア・ディジタル・コンテンツ電子配布システム100で使用することができる。音楽の場合、MPEG 1／2／4、Dolby AC－2およびAC－3、SonyのAdaptive Transform Coding(ATRAC)、および低ビット・レート・アルゴリズムが、典型的に使用される圧縮アルゴリズムの一部である。コンテンツ113は、記憶サイズ要件を減らすために、圧縮形式でエンドユーザ装置109に記憶される。コンテンツ113は、アクティブ再生中に圧縮解除される。スクランブル解除も、アクティブ再生中に実行される。スクランブル化の目的および種類は、後にコンテンツ使用制御層505の説明で記述する。
【0081】2. コンテンツ使用制御層505コンテンツ使用制御層505は、エンドユーザ装置109でのコンテンツ113の使用に課せられる条件または制約の指定と実施を可能にする。条件では、コンテンツ113の許可される再生回数、コンテンツ113の2次コピーが許可されるかどうか、2次コピーの回数、および、コンテンツ113を外部ポータブル装置にコピーすることができるかどうかを指定することができる。コンテンツ・プロバイダ101は、許容可能な使用条件517を設定し、これをSC内で電子ディジタル・コンテンツ商店103に送信する(ライセンス制御層501の節を参照されたい)。電子ディジタル・コンテンツ商店103は、コンテンツ・プロバイダ101によって設定されたオリジナルの条件を侵害しない限り、使用条件517を追加するか狭めることができる。電子ディジタル・コンテンツ商店103は、すべての商店使用条件519を(SC内で)エンドユーザ装置109およびクリアリングハウス105に送信する。クリアリングハウス105は、コンテンツ113のエンドユーザ装置109への公開を許可する前に、使用条件検証521を実行する。
【0082】コンテンツの使用条件517の実施は、エンドユーザ装置109のコンテンツ使用制御層505によって実行される。第1に、コンテンツ113の受信時に、エンドユーザ装置109のコンテンツ識別層503からのコピーによって、最初のコピー／再生許可を表すコピー／再生コード523を用いてコンテンツ113にマークがつけられる。第2に、プレイヤ・アプリケーション195が、コンテンツ113をエンドユーザ装置109に格納する前に、暗号的にコンテンツ113をスクランブルする。プレイヤ・アプリケーション195は、コンテンツ項目ごとにスクランブル化鍵を生成し、この鍵は、暗号化され、エンドユーザ装置109に隠される。その後、エンドユーザ装置109がコピーまたは再生のためにコンテンツ113にアクセスするたびに、エンドユーザ装置109は、コンテンツ113のスクランブル解除および再生またはコピーの実行を許可する前に、コピー／再生コードを検証する。エンドユーザ装置109は、コンテンツ113の元のコピーおよび新しい2次コピーのすべてのコピー／再生コードを適当に更新する。コピー／再生コーディングは、圧縮されているコンテンツ113に対して実行される。すなわち、コピー／再生コードを埋め込む前にコンテンツ113を圧縮解除する必要はない。
【0083】エンドユーザ装置109は、ライセンス透かし527を使用して、コンテンツ113にコピー／再生コードを埋め込む。埋込みアルゴリズムおよび関連するスクランブル化鍵を知っているエンドユーザ・プレイヤ・アプリケーション195だけが、埋め込まれたデータの読取または変更を行うことができる。このデータは、人間の観察者が見ることも聞くこともできない、すなわち、このデータは、コンテンツ113に知覚可能な劣化を導入しない。透かしは、コンテンツ処理の複数のステップ、データ圧縮、ディジタル・アナログ変換、アナログ・ディジタル変換、および通常のコンテンツ処理によって導入される信号劣化に耐えるので、透かしは、アナログ表現を含めてすべての表現形式のコンテンツ113に伴う。代替実施形態では、ライセンス透かし527を使用してコンテンツ113にコピー／再生コードを埋め込む代わりに、プレイヤ・アプリケーション195が、保護された形で格納された商店使用条件519を使用する。
【0084】3. コンテンツ識別層503コンテンツ識別層503の一部として、コンテンツ・プロバイダ101も、ライセンス透かし527を使用して、コンテンツ識別子、コンテンツ所有者、および公開日および地理的配布地帯などの他の情報などのデータを、コンテンツ113に埋め込む。この透かしを、著作権透かし529と称する。受信時に、エンドユーザ装置109は、コンテンツ購入者の名前およびトランザクションID535(下のライセンス制御層501の節を参照)と、ライセンスの日付および使用条件517などの他の情報を用いて、コンテンツ113のコピーにウォーターマーキングする。この透かしを、本明細書ではライセンス透かしと称する。コンテンツ113

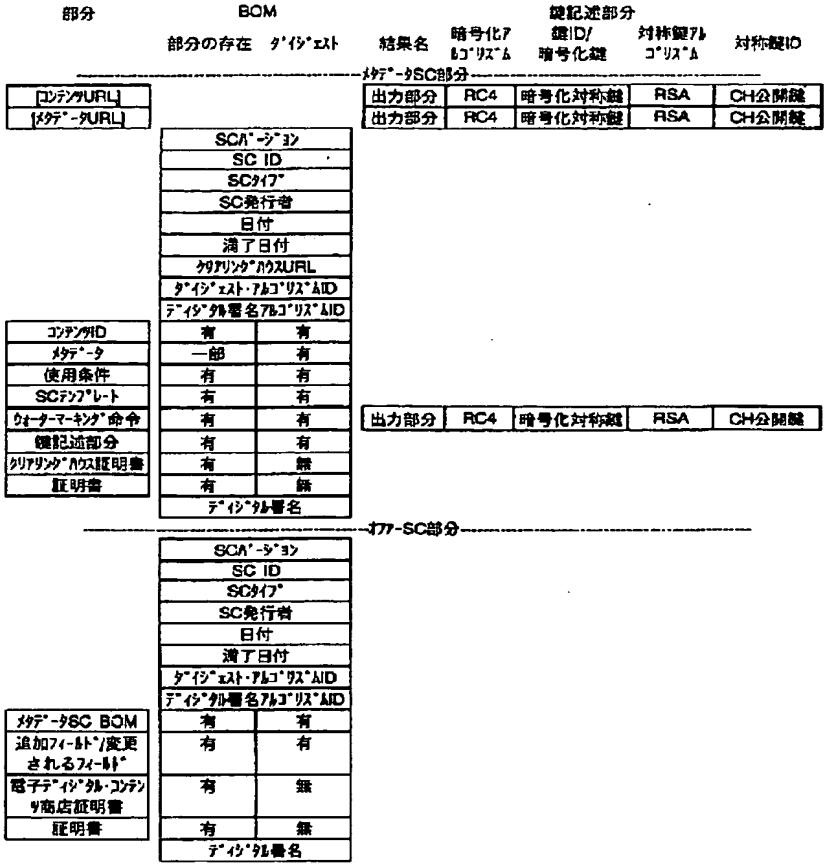
のコピーは、許可された形で得られたものであれ許可されない形で得られたものであれ、コンテンツ品質を保存するオーディオ処理の対象になり、著作権透かしおよびライセンス透かしを担持する。コンテンツ識別層503は、海賊行為を抑止する。
【0085】4. ライセンス制御層501ライセンス制御層501は、許可されない傍受からコンテンツ113を保護し、正しくライセンスを交付されたエンドユーザ装置109を有し、許可された電子ディジタル・コンテンツ商店103とのライセンス購入トランザクションを成功裡に完了したエンドユーザに個人単位でのみコンテンツが公開されることを保証する。ライセンス制御層501は、二重の暗号化531によってコンテンツ113を保護する。コンテンツ113は、コンテンツ・プロバイダ101によって生成された暗号化対称鍵を使用して暗号化され、この対称鍵は、クリアリングハウスの公開鍵621を使用して暗号化される。当初は、クリアリングハウス105だけが、対称鍵を回復することができる。
【0086】ライセンス制御は、「信頼される当事者」としてクリアリングハウス105を用いて設計されている。ライセンス要求537に対する許可(すなわち、エンドユーザ装置109へのコンテンツ113のための対称鍵623)の公開の前に、クリアリングハウス105は、トランザクション541およびライセンス許可543が完全であり、真正であることと、電子ディジタル・コンテンツ商店103が、電子的なコンテンツ113の販売に関するセキュア・ディジタル・コンテンツ電子配布システム100からの許可を有することと、エンドユーザが、正しくライセンスを交付されたアプリケーションを有することを検証する。監査／報告545によって、報告の生成と、セキュア・ディジタル・コンテンツ電子配布システム100内の他の許可された当事者とのライセンス交付トランザクション情報の共用が可能になる。
【0087】ライセンス制御は、SC処理533を介して実施される。SCは、暗号化されたコンテンツ113および情報を、システム・オペレーション・コンポーネント(下のSCの詳細な構造の節を参照)の間で配布するのに使用される。SCは、暗号暗号化、ディジタル署名、およびディジタル証明書を使用して、電子情報またはコンテンツ113の許可されない傍受および変更に対する保護を提供する、情報の暗号担体である。SCは、電子データの認証性検証も可能にする。
【0088】ライセンス制御は、コンテンツ・プロバイダ101、電子ディジタル・コンテンツ商店103、およびクリアリングハウス105が、これらのコンポーネントの認証に使用される信頼できる認証機関からの真正の暗号ディジタル証明書を有することを必要とする。エンドユーザ装置109は、ディジタル証明書を有する必要がない。
【0089】C. コンテンツ配布およびライセンス交付制御図9は、図8のライセンス制御層に適用されるコンテンツ配布およびライセンス交付制御の概要を示すブロック図である。この図には、電子ディジタル・コンテンツ商店103、エンドユーザ装置109、およびクリアリングハウス105が、インターネットを介して相互接続され、ユニキャスト(2地点間)伝送がこれらのコンポーネントの間で使用される場合が示されている。コンテンツ・プロバイダ101と電子ディジタル・コンテンツ商店103の間の通信は、インターネットまたは他のネットワークを介することもできる。エンドユーザ装置109と電子ディジタル・コンテンツ商店103の間のコンテンツ購入商取引トランザクションは、標準インターネット・ウェブ・プロトコルに基づくと仮定する。ウェブベース対話の一部として、エンドユーザは、購入するコンテンツ113の選択を行い、個人情報および会計情報を供給し、購入の条件に同意する。電子ディジタル・コンテンツ商店103は、SETなどのプロトコルを使用して、獲得機関から支払許可を得ることができる。
【0090】図9では、電子ディジタル・コンテンツ商店103が、標準ウェブ・プロトコルに基づいて、エンドユーザ装置109にプレイヤ・アプリケーション195をダウンロード済みであることも仮定する。このアーキテクチャは、電子ディジタル・コンテンツ商店103が、ダウンロードされたプレイヤ・アプリケーション195に一意のアプリケーションIDを割り当て、エンドユーザ装置109が、それを後のアプリケーション・ライセンス検証(下を参照)のために記憶することを必要とする。
【0091】全体的なライセンス交付のフローは、コンテンツ・プロバイダ101から始まる。コンテンツ・プロバイダ101は、ローカルに生成された暗号化対称鍵を使用してコンテンツ113を暗号化し、クリアリングハウス105の公開鍵621を使用して対称鍵623を暗号化する。代替実施形態では、対称鍵を、ローカルに生成する代わりに、クリアリングハウス105からコンテンツ・プロバイダ101に送信することができる。コンテンツ・プロバイダ101は、暗号化されたコンテンツ113を囲むコンテンツSC630と、暗号化された対称鍵623、商店使用条件519、および他のコンテンツ113関連情報を囲むメタデータSC620とを作成する。すべてのコンテンツ113オブジェクトについて、1つのメタデータSC620および1つのコンテンツSC630がある。コンテンツ113オブジェクトは、同一の曲の1つの圧縮レベルとするか、アルバムの各曲とするか、アルバム全体とすることができる。コンテンツ113オブジェクトごとに、メタデータSC620も、コンテンツ使用制御層505に関連する商店使用条件519を担持する。
【0092】コンテンツ・プロバイダ101は、1つまたは複数の電子ディジタル・コンテンツ商店103にメタデータSC620を配布し(ステップ601)、1つまたは複数のコンテンツ・ホスティング・サイトにコンテンツSC630を配布する(ステップ602)。各電子ディジタル・コンテンツ商店103は、オファーSC641を作成する。オファーSC641は、通常は、コンテンツ・プロバイダ101のディジタル署名624とディジタル証明書(コンテンツ・プロバイダ101については図示せず)を含む、メタデータSC620とほぼ同一の情報を担持する。上で述べたように、電子ディジタル・コンテンツ商店103は、当初はコンテンツ・プロバイダ101によって定義される商店使用条件519(コンテンツ使用制御層によって処理される)を追加するか狭めることができる。任意選択として、コンテンツSC630またはメタデータSC620もしくはその両方に、コンテンツ・プロバイダ101のディジタル署名624を用いて署名することができる。
【0093】エンドユーザ装置109と電子ディジタル・コンテンツ商店103のコンテンツ購入トランザクション(ステップ603)の完了の後に、電子ディジタル・コンテンツ商店103は、トランザクションSC640を作成し、エンドユーザ装置109に転送する(ステップ604)。トランザクションSC640には、一意のトランザクションID535、購入者の名前(すなわちエンドユーザの名前)(図示せず)、エンドユーザ装置109の公開鍵661、および購入されたコンテンツ113に関連するオファーSC641が含まれる。図9のトランザクション・データ642は、トランザクションID535とエンドユーザ名(図示せず)の両方を表す。トランザクション・データ642は、クリアリングハウス105の公開鍵621を用いて暗号化される。任意選択として、トランザクションSC640に、電子ディジタル・コンテンツ商店103のディジタル署名643を用いて署名する。
【0094】トランザクションSC640(およびそれに含まれるオファーSC641)の受信時に、エンドユーザ装置109上で稼動するプレイヤ・アプリケーション195が、注文SC650によってクリアリングハウス105にライセンス許可の送信を請求する(ステップ605)。注文SC650には、オファーSC641からの暗号化された対称鍵623および商店使用条件519、トランザクションSC640からの暗号化されたトランザクション・データ642、およびエンドユーザ装置109からの暗号化されたアプリケーションID551が含まれる。もう1つの実施形態では、注文SC650が、エンドユーザ装置109のディジタル署名652を用いて署名される。
【0095】エンドユーザ装置109からの注文SC650の受信時に、クリアリングハウス105は、下記を検証する。
1. 電子ディジタル・コンテンツ商店103が、セキュア・ディジタル・コンテンツ電子配布システム100からの許可を有する(クリアリングハウス105のデータベース160内に存在する)こと2. 注文SC650が変更されていないこと3. トランザクション・データ642および対称鍵623が完全であり、真正であること4. エンドユーザ装置109によって購入された電子商店使用条件519が、コンテンツ・プロバイダ101によって設定された使用条件517との一貫性を有すること5. アプリケーションID551が有効な構造を有し、許可された電子ディジタル・コンテンツ商店103によって供給されたものであること【0096】検証が成功である場合には、クリアリングハウス105は、対称鍵623およびトランザクション・データ642を解読し、ライセンスSC660を作成し、エンドユーザ装置109に転送する(ステップ606)。ライセンスSC660は、対称鍵623およびトランザクション・データ642を担持し、この両方が、エンドユーザ装置109の公開鍵661を使用して暗号化されている。検証が成功でない場合には、クリアリングハウス105は、エンドユーザ装置109へのライセンスを拒否し、エンドユーザ装置109に知らせる。クリアリングハウス105は、即座に、この検証失敗について電子ディジタル・コンテンツ商店103にも知らせる。代替実施形態では、クリアリングハウス105は、そのディジタル署名663を用いてラ

イセンスSC660に署名する。
【0097】ライセンスSC660を受信した後に、エンドユーザ装置109は、前にクリアリングハウス105から受信した対称鍵623およびトランザクション・データ642を解読し、コンテンツ・ホスティング・サイト111にコンテンツSC630を要求する(ステップ607)。コンテンツSC630の到着時(ステップ608)に、エンドユーザ装置109は、対称鍵623を使用してコンテンツ113を解読し(ステップ609)、コンテンツ113およびトランザクション・データ642を、ライセンス・ウォーターマーキング、コピー／再生コーディング、スクランブル化、および図8に関して前に説明したコンテンツ113の他の処理のための層に渡す。
【0098】最後に、クリアリングハウス105は、周期的に、監査および追跡のために、コンテンツ・プロバイダ101および電子ディジタル・コンテンツ商店103に要約トランザクション報告を送信する(ステップ610)。
【0099】V. セキュア・コンテナの構造A. 全般的な構造セキュア・コンテナ(SC)は、一緒にコンテンツ113の単位またはトランザクションの一部を定義し、使用条件、メタデータ、および暗号化方法などの関連情報も定義する、複数の部分からなる構造である。SCは、情報の保全性、完全性、および認証性を検証できる形で設計されている。SC内の情報の一部は、暗号化し、その結果、正しい許可が得られた後でなければアクセスできないようにすることができる。
【0100】SCには、SCに関する情報およびSCに含まれる部分のそれぞれに関する情報の記録を有する少なくとも1つの材料表(BOM)部分が含まれる。メッセージ・ダイジェストが、部分ごとに、MD－5などのハッシュ・アルゴリズムを使用して計算され、その部分のBOMレコードに含まれる。部分のダイジェストは、互いに連結され、それからもう1つのダイジェストが計算され、SCを作成する実体の秘密鍵を使用して暗号化されて、ディジタル署名が作成される。SCを受け取る当事者は、このディジタル署名を使用して、ダイジェストのすべてを検証することができ、したがって、SCおよびそのすべての部分の保全性および完全性を検証することができる。
【0101】下記の情報を、各部分のレコードと共にBOM内のレコードとして含めることができる。SCのタイプによって、どのレコードを含める必要があるかが決定される。
・SCバージョン・SC ID・SCタイプ(たとえば、オファー、注文、トランザクション、コンテンツ、メタデータまたは販売促進、およびライセンス)
・SC発行者・SC作成日付・SC満了日付・クリアリングハウスのURL・含まれる部分に使用されたダイジェスト・アルゴリズムの記述(デフォルトはMD－5)
・ディジタル署名暗号化に使用されたアルゴリズムの記述(デフォルトはRSA)
・ディジタル署名(含まれる部分の連結されたダイジェストのすべての暗号化されたダイジェスト)
【0102】SCには、複数のBOMを含めることができる。たとえば、オファーSC641は、そのBOMを含むオリジナルのメタデータSC620部分、ならびに電子ディジタル・コンテンツ商店103によって追加された追加情報および新規BOMからなる。メタデータSC620のBOMのレコードは、オファーSC641のBOMに含まれる。このレコードには、その保全性を検証するのに使用することができるメタデータSC620のBOMのダイジェストが含まれ、したがって、メタデータSC620から含まれる部分の保全性も、メタデータSC620のBOMに格納された部分ダイジェスト値を使用して検証することができる。メタデータSC620からの部分のすべてが、オファーSC641のために作成された新しいBOM内のレコードを有しない。電子ディジタル・コンテンツ商店103およびメタデータSC620のBOMによって追加される部分だけが、新しいBOM内のレコードを有する。
【0103】SCには、鍵記述部分も含めることができる。鍵記述部分には、SC内の暗号化された部分に関する下記の情報を含むレコードが含まれる。
・暗号化された部分の名前。
・解読された時にその部分に使用される名前。
・その部分の暗号化に使用された暗号化アルゴリズム。
・その部分の暗号化に使用された公開暗号化鍵を示す鍵識別子、または、解読された時に暗号化された部分の解読に使用される暗号化された対称鍵のいずれか。
・対称鍵の暗号化に使用された暗号化アルゴリズム。このフィールドは、鍵記述部分のレコードに、暗号化された部分の暗号化に使用された暗号化された対称鍵が含まれる時に限って存在する。
・対称鍵の暗号化に使用された公開暗号化鍵の鍵識別子。このフィールドは、鍵記述部分のレコードに暗号化された対称鍵と、暗号化された部分の暗号化に使用された対称鍵の暗号化アルゴリズム識別子が含まれる時に限って存在する。
【0104】SCに暗号化された部分が含まれない場合、鍵記述部分はない。
【0105】B. 権利管理言語の構文およびセマンティクス権利管理言語は、コンテンツ113購入後にエンドユーザがコンテンツ113の使用に関する制限を定義する値を割り当てることができるパラメータからなる。コンテンツ113の使用に関する制限は、使用条件517である。各コンテンツ・プロバイダ101は、そのコンテンツ113項目のそれぞれについて使用条件517を指定する。電子ディジタル・コンテンツ商店103は、メタデータSC620内の使用条件517を解釈し、その情報を使用して、顧客に提供したい選択肢を提供し、コンテンツ113の小売り購入情報を追加する。エンドユーザが購入のためにコンテンツ113項目を選択した後に、エンドユーザ装置109は、商店使用条件519に基づいてコンテンツ113の許可を要求する。クリアリングハウス105は、エンドユーザにライセンスSC660を送信する前に、要求された商店使用条件519が、コンテンツ・プロバイダ101によってメタデータSC620内で指定された許容可能な使用条件517に一致することを検証する。
【0106】エンドユーザ装置109が、購入したコンテンツ113を受信した時に、商店使用条件519が、ウォーターマーキング・ツールを使用してコンテンツ113内に符号化されるか、保護された形で格納される商店使用条件519内で符号化される。エンドユーザ装置109で稼動するプレイヤ・アプリケーション195が、コンテンツ113に符号化された商店使用条件519が実施されることを保証する。
【0107】下記が、コンテンツ113が音楽である場合の実施形態の商店使用条件519の例である。
・曲が記録可能である。
・曲をn回再生することができる。
【0108】C. セキュア・コンテナのフローおよび処理の概要メタデータSC620は、コンテンツ・プロバイダ101によって作成され、曲などのコンテンツ113項目の定義に使用される。コンテンツ113自体は、これらのSCに含まれない。というのは、コンテンツ113のサイズが、通常は、電子ディジタル・コンテンツ商店103およびエンドユーザが説明的なメタデータにアクセスする目的だけのためにコンテナを効率的にダウンロードするには大きすぎるからである。その代わりに、このSCには、コンテンツ113を指す外部URL(Uniform Resource Locator)が含まれる。SCには、曲のコンテンツ113の場合に音楽、CDカバー・アート、またはディジタル・オーディオ・クリップなどの、コンテンツ113に関する説明的な情報および他の関連データを提供するメタデータも含まれる。
【0109】電子ディジタル・コンテンツ商店103は、許可されるメタデータSC620をダウンロードし、オファーSC641を作成する。手短に言うと、オファーSC641は、メタデータSC620からの部分およびBOMのいくつかと、電子ディジタル・コンテンツ商店103によって含められる追加情報からなる。オファーSC641の新規BOMは、オファーSC641を作成する時に作成される。また、電子ディジタル・コンテンツ商店103は、メタデータSC620からメタデータ情報を抽出して、通常はエンドユーザがコンテンツ113を購入できるように、エンドユーザへのコンテンツ113の記述を表すウェブ・サイト上のHTMLページを作成することによって、メタデータSC620を使用する。

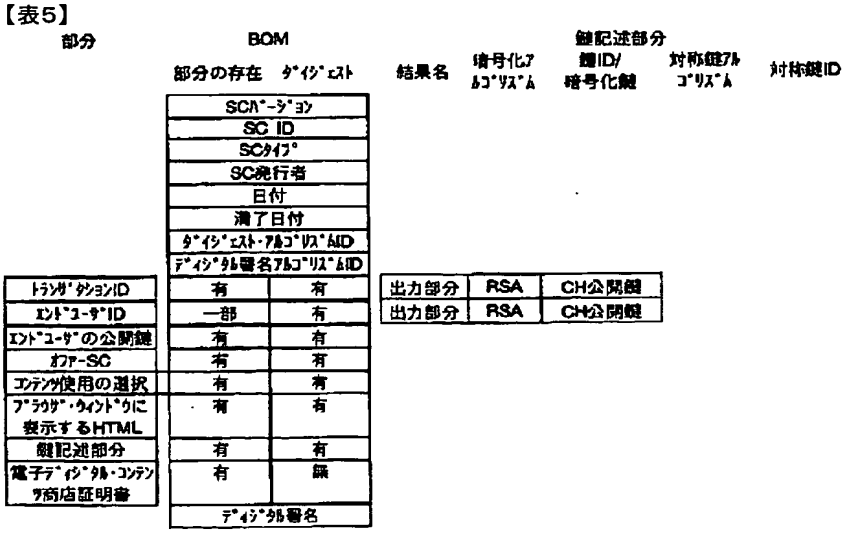
【0110】電子ディジタル・コンテンツ商店103によって追加されるオファーSC641内の情報は、通常は、メタデータSC620で指定される使用条件517の選択を狭めるためのものと、その商店のロゴのグラフィック・イメージ・ファイルおよびその商店のウェブ・サイトへのURLなどの販売促進データである。メタデータSC620内のオファーSC641テンプレートが、オファーSC641内で電子ディジタル・コンテンツ商店103が変更できる情報と、電子ディジタル・コンテンツ商店103に必要な追加情報がある場合にはその情報と、埋め込まれるメタデータSC620内で保持される部分を示す。
【0111】オファーSC641は、エンドユーザが電子ディジタル・コンテンツ商店103からのコンテンツ113の購入を決定した時に、トランザクションSC640に含められる。電子ディジタル・コンテンツ商店103は、トランザクションSC640を作成し、購入されるコンテンツ113項目ごとにオファーSC641を含め、エンドユーザ装置109に送信する。エンドユーザ装置109は、トランザクションSC640を受信し、トランザクションSC640および含まれるオファーSC641の保全性を検証する。
【0112】注文SC650は、購入されるコンテンツ113項目ごとにエンドユーザ装置109によって作成される。オファーSC641からの情報、トランザクションSC640からの情報、およびエンドユーザ装置109の構成ファイルからの情報が含まれる。注文SC650は、1時に1つずつ、クリアリングハウス105に送信される。注文SC650が送信される先のクリアリングハウス105のURLは、メタデータSC620のBOM内にレコードの1つとして含まれ、オファーSC641にも含まれる。
【0113】クリアリングハウス105は、注文SC650を検証し、処理して、ライセンス透かし527と購入したコンテンツ113へのアクセスとに必要なすべてのものをエンドユーザ装置109に供給する。クリアリングハウス105の機能の1つが、オファーSC641からウォーターマーキング命令を解読し、コンテンツSC630からコンテンツ113を解読するのに必要な対称鍵623の解読である。暗号化された対称鍵623のレコードには、実際には、実際の暗号化された対称鍵623以上のものが含まれる。暗号化を実行する前に、コンテンツ・プロバイダ101は、任意選択として、その名前を実際の対称鍵623に付加することができる。コンテンツ・プロバイダ101の名前を対称鍵623と一緒に暗号化することによって、合法的なSCからそれ自体のメタデータSC620およびコンテンツSC630を作成する海賊のコンテンツ・プロバイダ101に対するセキュリティが提供される。クリアリングハウス105は、対称鍵623と一緒に暗号化されたコンテンツ・プロバイダ101の名前が、SC証明書のコンテンツ・プロバイダ101の名前と一致することを検証する。
【0114】クリアリングハウス105によるウォーターマーキング命令に対して行う必要がある変更がある場合には、クリアリングハウス105は、対称鍵623を解読し、ウォーターマーキング命令を変更し、新しい対称鍵623を使用してそのウォーターマーキング命令をもう一度暗号化する。この対称鍵623は、エンドユーザ装置109の公開鍵661を使用して再暗号化される。クリアリングハウス105は、SCの他の対称鍵623も解読し、エンドユーザ装置109の公開鍵661を用いてもう一度暗号化する。クリアリングハウス105は、注文SC650に応答して、新たに暗号化された対称鍵623と更新されたウォーターマーキング命令を含むライセンスSC660を作成し、エンドユーザ装置109に送信する。注文SC650の処理が完全に成功ではない場合には、クリアリングハウス105は、許可処理の失敗について知らせるHTMLページまたは同等物をエンドユーザ装置109に返す。
【0115】ライセンスSC660は、コンテンツ113項目へのアクセスに必要なすべてのものをエンドユーザ装置109に提供する。エンドユーザ装置109は、コンテンツ・ホスティング・サイト111に、適当なコンテンツSC630を要求する。コンテンツSC630は、コンテンツ・プロバイダ101によって作成され、これには、暗号化されたコンテンツ113部分とメタデータ部分が含まれる。プレイヤ・アプリケーション195は、ライセンスSC660からの対称鍵623を使用して、コンテンツ113、メタデータ、およびウォーターマーキング命令を解読する。その後、ウォーターマーキング命令が、コンテンツ113に添付され、コンテンツ113が、スクランブル化され、エンドユーザ装置109に記憶される。
【0116】D. メタデータ・セキュア・コンテナ620のフォーマット下の表に、メタデータSC620に含まれる諸部分を示す。「部分」列の箱のそれぞれは、BOMと共にSCに含まれる別々のオブジェクトである([]文字によって囲まれた部分名を除く)。BOMには、SCに含まれる部分ごとに1つのレコードが含まれる。「部分の存在」列には、その部分自体が実際にSCに含まれるかどうかが示され、「ダイジェスト」列には、その部分についてメッセージ・ダイジェストが計算されるかどうかが示される。いくつかの部分は、SCが他のSCに含まれる時に伝播されない場合がある(関連するテンプレートによって決定される)が、オリジナルのBOM全体は伝播される。これは、オリジナルのSCに含まれるディジタル署名を検証するために、クリアリングハウス105がBOM全体を必要とするからである。
【0117】下の表の「鍵記述部分」列では、SCの鍵記述部分に含まれるレコードが定義される。鍵記述部分のレコードによって、SC内の部分または別のSC内の部分の暗号化に使用された暗号化鍵および暗号化アルゴリズムに関する情報が定義される。各レコードには、暗号化された部分の名前と、必要な場合にはその暗号化された部分に含まれる別のSCを指すURLが含まれる。「結果名」列では、解読の後にその部分に割り当てられる名前が定義される。「暗号化アルゴリズム」列では、その部分の暗号化に使用された暗号化アルゴリズムが定義される。「鍵ID／暗号化鍵」列では、その部分の暗号化に使用された暗号化鍵の識別か、その部分の暗号化に使用された暗号化された対称鍵623のビット列のbase64符号化のいずれかが定義される。「対称鍵アルゴリズム」列は、前の列が暗号化された対称鍵623である時に、対称鍵623の暗号化に使用された暗号化アルゴリズムを定義する任意選択のパラメータである。「対称鍵ID」列は、「鍵ID／暗号化鍵」列が暗号化された対称鍵623である時に、対称鍵623の暗号化に使用された暗号化鍵の識別である。
【0118】
【表3】



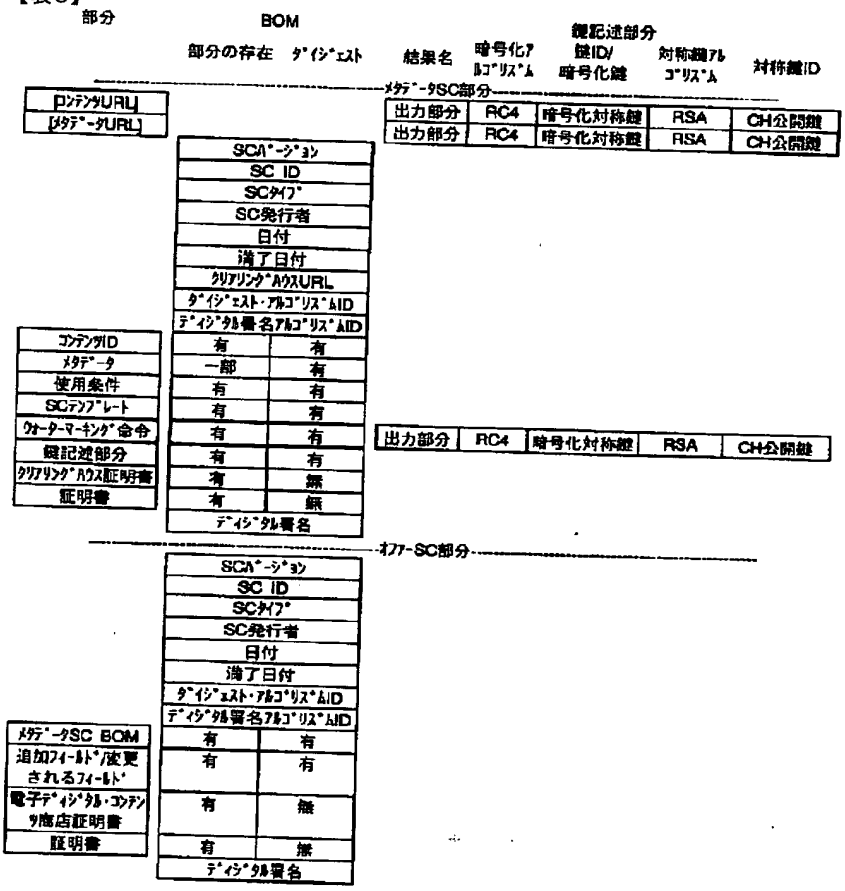
【0119】下で、上のメタデータSCの表で使用する用語を説明する。
・[コンテンツURL] 鍵記述部分のレコード内のパラメータ。これは、このメタデータSC620に関連するコンテンツSC630内の暗号化されたコンテンツ113を指すURLである。メタデータSC620自体には、暗号化されたコンテンツ113が含まれない。
・[メタデータURL] 鍵記述部分のレコード内のパラメータ。これは、このメタデータSC620に関連するコンテンツSC630内の暗号化されたメタデータを指すURLである。メタデータSC620自体には、暗号化されたメタデータが含まれない。
・コンテンツID コンテンツ113項目に割り当てられた一意のIDを定義する部分。メタデータSC620が複数のコンテンツ113項目を参照する場合には、この部分に複数のコンテンツIDが含まれる。
・メタデータ 曲の場合にはアーティスト名およびCDカバー・アートなどのコンテンツ113項目に関連する情報を含む部分。複数のメタデータ部が存在する場合があり、そのうちのいくつかが暗号化されている場合がある。メタデータ部分の内部構造は、そこに含まれるメタデータのタイプに依存する。
・使用条件 コンテンツ113の使用に関してエンドユーザに課せられる使用のオプション、規則、および制約を記述する情報を含む部分。
・SCテンプレート オファーSC、注文SC、およびライセンスSC660の作成に必要な情報および任意選択の情報を記述するテンプレートを定義する部分。
・ウォーターマーキング命令 コンテンツ113内でウォーターマーキングを実施するための暗号化された命令およびパラメータを含む部分。ウォーターマーキング命令は、クリアリングハウス105によって変更され、ライセンスSC660内でエンドユーザ装置109に返される場合がある。鍵記述部分に、ウォーターマーキング命令を暗号化するのに使用された暗号化アルゴリズム、ウォーターマーキング命令が解読される時に使用される出力部分の名前、ウォーターマーキング命令の暗号化に使用された暗号化された対称鍵623のビット列のbase64符号化、対称鍵623の暗号化に使用された暗号化アルゴリズム、および対称鍵623の解読に必要な公開鍵の識別を定義するレコードがある。
・クリアリングハウス証明書 クリアリングハウス105の署名された公開鍵621を含む、証明機関またはクリアリングハウス105からの証明書。証明書が複数ある場合があり、その場合には、階層レベル構造が使用され、最上位の証明書に、次のレベルの証明書をオープンするための公開鍵が含まれ、最下位レベルの証明書に達すると、クリアリングハウス105の公開鍵621が含まれている。
・証明書 SCを作成した実体の署名された公開鍵621を含む、認証機関またはクリアリングハウス105からの証明書。証明書が複数ある場合があり、その場合には、階層レベル構造が使用され、最上位の証明書に、次のレベルの証明書をオープンするための公開鍵が含まれ、最下位レベルの証明書に達すると、SC作成者の公開鍵が含まれている。
・SCバージョン SCパッカー・ツールによってSCに割り当てられるバージョン番号。
・SC ID SCを作成した実体によってSCに割り当てられる一意のID。
・SCタイプ SCのタイプ(たとえばメタデータ、オファー、注文など)を示す。
・SC発行者 SCを作成した実体を示す。
・作成日付 SCが作成された日付。
・満了日付 SCが満了し、もはや有効でなくなる日付。
・クリアリングハウスURL プレイヤ・アプリケーション195が、コンテンツ113にアクセスするための正しい許可を得るために対話しなければならないクリアリングハウス105のアドレス。
・ダイジェスト・アルゴリズムID 諸部分のダイジェストを計算するのに使用されたアルゴリズムの識別子。
・ディジタル署名アルゴリズムID 連結された部分ダイジェストのダイジェストを暗号化するのに使用されたアルゴリズムの識別子。この暗号化された値がディジタル署名である。
・ディジタル署名 SCを作成した実体の公開鍵を用いて暗号化された、連結された部分ダイジェストのダイジェスト。
・出力部分 暗号化された部分が解読された時に出力部分に割り当てられる名前。
・RSAおよびRC4 対称鍵623およびデータ部分の暗号化に使用されるデフォルトの暗号化アルゴリズム。
・暗号化対称鍵 解読された時に、SC部分の解読に使用される、暗号化された鍵のビット列のbase64符号化。
・CH公開鍵 クリアリングハウス105の公開鍵621がデータの暗号化に使用されたことを示す識別子。
【0120】E. オファー・セキュア・コンテナ641のフォーマット下の表に、オファーSC641に含まれる部分を示す。メタデータ部分の一部を除く部分および、メタデータSC620からのBOMは、オファーSC641にも含まれる。
【0121】
【表4】



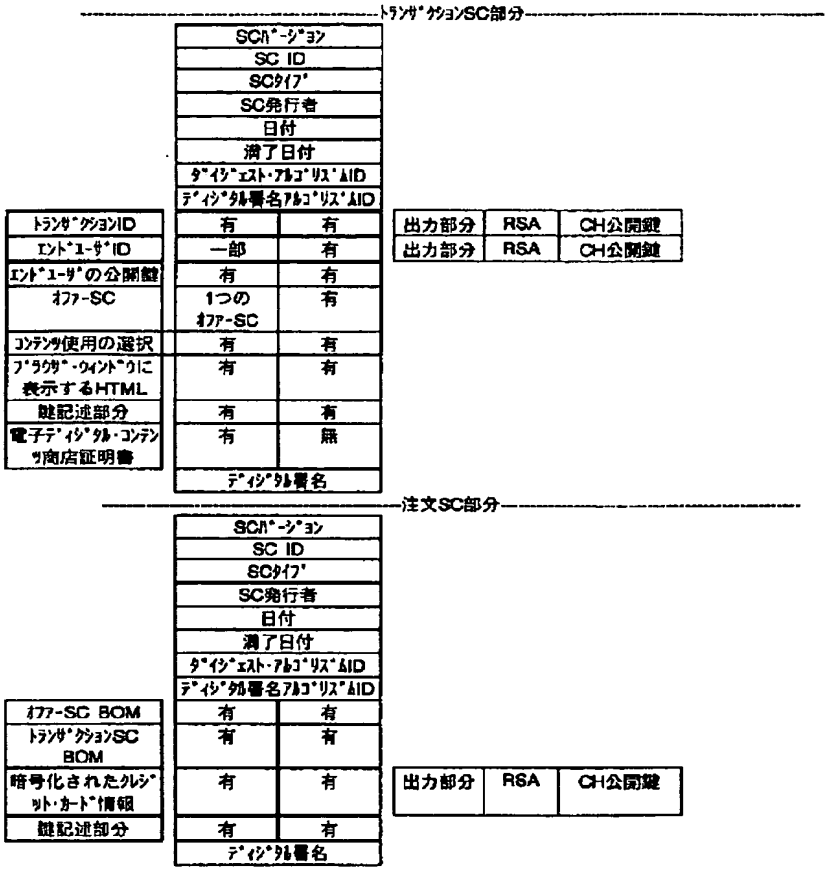
【0122】下で、上のオファーSC641で使用されている、別のSCについて前に説明されなかった用語を説明する。
・メタデータSC BOM オリジナルのメタデータSC620からのBOM。オファーSC641のBOMのレコードには、メタデータSC620のBOMのダイジェストが含まれる。
・追加フィールド／変更されるフィールド 電子ディジタル・コンテンツ商店103によって変更された使用条件情報。この情報は、電子ディジタル・コンテンツ商店103が変更したもののすべてがその許可の範囲内であることを確認するために、受信したSCテンプレートによって、クリアリングハウス105によって検証される。
・電子ディジタル・コンテンツ商店証明書 クリアリングハウス105によって電子ディジタル・コンテンツ商店103に供給され、クリアリングハウス105の秘密鍵を使用してクリアリングハウス105によって署名された証明書。この証明書は、プレイヤ・アプリケーション195によって、電子ディジタル・コンテンツ商店103がコンテンツ113の有効なディストリビュータであることを検証するのに使用される。プレイヤ・アプリケーション195およびクリアリングハウス105は、クリアリングハウス105の公開鍵621を用いて証明書の署名を解読することによって、電子ディジタル・コンテンツ商店103が許可されたディストリビュータであることを検証することができる。プレイヤ・アプリケーション195は、インストール中の初期設定の一部として受信したクリアリングハウス105の公開鍵621のローカル・コピーを保存する。
【0123】F. トランザクション・セキュア・コンテナ640のフォーマット下の表に、トランザクションSC640ならびにそのBOM部分および鍵記述部分に含まれる部分を示す。
【0124】
【表5】



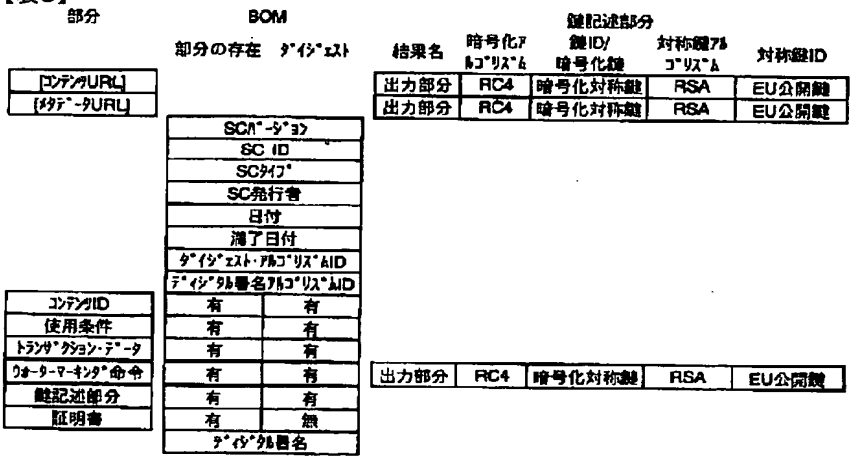
【0125】下で、上のトランザクションSC640で使用されている、別のSCについて前に説明しなかった用語を説明する。
・トランザクションID535 トランザクションを一意に識別するために電子ディジタル・コンテンツ商店103によって割り当てられるID。
・エンドユーザID エンドユーザが購入選択を行い、クレジット・カード情報を提供する時に電子ディジタル・コンテンツ商店103が得るエンドユーザの識別。
・エンドユーザの公開鍵 対称鍵623を再暗号化するのにクリアリングハウス105が使用する、エンドユーザの公開鍵661。エンドユーザの公開鍵661は、購入トランザクション中に電子ディジタル・コンテンツ商店103に送信される。
・オファーSC 購入されたコンテンツ113項目に関するオファーSC641。
・コンテンツ使用の選択 エンドユーザによって購入されるコンテンツ113項目ごとの使用条件の配列。オファーSC641ごとに1つの項目がある。
・表示するHTMLトランザクションSC640の受信時またはエンドユーザ装置109とクリアリングハウス105の間の対話中に、インターネット・ブラウザ・ウィンドウ内にプレイヤ・アプリケーション195が表示する1つまたは複数のHTMLページ。
【0126】エンドユーザ装置109がトランザクションSC640を受信した時に、SCの保全性および認証性を検証するために、次のステップを実行することができる。
1. クリアリングハウス105の公開鍵621を使用して、電子ディジタル・コンテンツ商店103の証明書の保全性を検証する。クリアリングハウス105の公開鍵621は、プレイヤ・アプリケーション195のインストール中にプレイヤ・アプリケーション195の初期設定の一部として受信された後に、エンドユーザ装置109に記憶される。
2. 電子ディジタル・コンテンツ商店103証明書からの公開鍵を使用して、SCのディジタル署名643を検証する。
3. SCの諸部分のハッシュを検証する。
4. トランザクションSC640に含まれるオファーSC641のそれぞれの保全性および認証性を検証する。
【0127】G. 注文セキュア・コンテナ650のフォーマット次の表に、注文SC650ならびにそのBOM部分および鍵記述部分に含まれる部分を示す。これらの部分は、解読および検証の目的のためにクリアリングハウス105に情報を提供するか、クリアリングハウス105によって検証されるかのいずれかである。オファーSC641からの部分およびBOMは、注文SC650にも含まれる。メタデータSCのBOMの「部分の存在」列の「一部」は、これらの部分の一部が注文SC650に含まれないことを示す。メタデータSC620からのBOMも、変更無しで含まれ、その結果、クリアリングハウス105が、メタデータSC620およびその諸部分の保全性を検証できるようになる。
【0128】
【表6】



【表7】



【0129】下で、上の注文SC650で使用されている、別のSCについて前に説明しなかった用語を説明する。
・トランザクションSC BOM オリジナルのトランザクションSC640のBOM。注文SC650のBOM内のレコードには、トランザクションSC640のBOMのダイジェストが含まれる。
・暗号化されたクレジット・カード情報 クレジット・カードまたはデビット・カードに購入額を請求するのに使用される、エンドユーザからの任意選択の暗号化された情報。この情報は、オファーSC641を作成した電子ディジタル・コンテンツ商店103が、顧客への請求を処理しない時(この場合、クリアリングハウス105が請求を処理することができる)に必要になる。
【0130】H. ライセンス・セキュア・コンテナ660のフォーマット下の表に、ライセンスSC660ならびにそのBOMに含まれる部分を示す。鍵記述部分に示されているように、ウォーターマーキング命令、コンテンツ113、およびコンテンツ113メタデータの解読に必要な対称鍵623は、エンドユーザの公開鍵661を使用して、クリアリングハウス105によって再暗号化されている。エンドユーザ装置109は、ライセンスSC660の受信時に、対称鍵623を解読し、これらを使用して、ライセンスSC660およびコンテンツSC630からの暗号化された部分にアクセスする。
【0131】
【表8】



【0132】下で、上のライセンスSC660で使用されている、別のSCについて前に説明しなかった用語を説明する。
・EU公開鍵 エンドユーザの公開鍵661がデータの暗号化に使用されたことを示す識別子。
・注文SC650ID 注文SC650のBOMからとられたSC ID。
・証明書取消リスト 前に発行され、クリアリングハウス105によって署名されたが、もはや有効とは見なされない証明書IDの任意選択のリスト。取消リストに含まれる証明書によって検証できる署名を有するSCは、すべてが無効なSCである。プレイヤ・アプリケ

ーション195は、クリアリングハウス105の証明書取消リストのコピーをエンドユーザ装置109に記憶する。取消リストを受信した時には必ず、プレイヤ・アプリケーション195は、その取消リストがより新しい場合にローカル・コピーと置換する。取消リストには、どのリストが最も新しいかを判定するために、バージョン番号またはタイム・スタンプ(またはその両方)が含まれる。
【0133】I. コンテンツ・セキュア・コンテナのフォーマット下の表に、コンテンツSC630ならびにBOMに含まれる部分を示す。
【0134】
【表9】

部分	BOM 部分の存在 ﾀﾞｲｼﾞｪｽﾄ
	SCﾊﾞｰｼﾞｮﾝ
	SC ID
	SCﾀｲﾌﾟ
	SC発行者
	日付
	満了日付
	ｸﾘｱﾘﾝｸﾞﾊｳｽURL
	ﾀﾞｲｼﾞｪｽﾄ・ｱﾙｺﾞﾘｽﾞﾑID
	ﾃﾞｨｼﾞﾀﾙ署名ｱﾙｺﾞﾘｽﾞﾑID
ｺﾝﾃﾝﾂID	有 有
暗号化されたｺﾝﾃﾝﾂ	有 有
暗号化されたﾒﾀﾃﾞｰﾀ	有 有
ﾒﾀﾃﾞｰﾀ	有 有
証明書	有 無
	ﾃﾞｨｼﾞﾀﾙ署名

【0135】下で、上のコンテンツSC630で使用されている、別のSCについて前に説明しなかった用語を説明する。
・暗号化されたコンテンツ 対称鍵623を使用してコンテンツ・プロバイダ101によって暗号化されたコンテンツ113。
・暗号化されたメタデータ 対称鍵623を使用してコンテンツ・プロバイダ101によって暗号化された、コンテンツ113に関連するメタデータ。
【0136】暗号化された部分の解読に必要な鍵は、クリアリングハウス105で作成されるライセンスSC660内にあるので、コンテンツSC630には鍵記述部分が含まれない。
【0137】VI. セキュア・コンテナのパックとアンパックA. 概要SCパッカーは、指定された部分のすべてを用いてSCを作成するための複数ステップまたは単一ステップのいずれかの処理で呼び出すことができるAPI(アプリケーション・プログラミング・インターフェース)を有する32ビットWindowsプログラムである。SCパッカー・ツール151、152、および153は、コンテンツ・プロバイダ101、クリアリングハウス105、電子ディジタル・コンテンツ商店103、およびSCパッキングを必要とする他のサイトのWindowsプログラムをサポートするさまざまなハードウェア・プラットホームで稼動する。BOMと、必要な場合には鍵記述部分が、作成され、SCに含まれる。1組のパッカーAPIを用いて、呼出し元が、BOMおよび鍵記述部分のレコードを生成し、SCに諸部分を含めるのに必要な情報を指定することができる。諸部分および対称鍵623の暗号化ならびにダイジェストおよびディジタル署名の計算も、パッカーによって実行される。パッカーによってサポートされる暗号化アルゴリズムおよびダイジェスト・アルゴリズムは、パッカー・コードに含まれるか、外部インターフェースを介して呼び出される。
【0138】SCを作成するためのパッカーへのインターフェースは、入力として以下のパラメータを受け入れるAPIによって行われる。
・連結された構造体のバッファへのポインタ。バッファ内の各構造体は、コマンドを実行するのに必要な情報を含む、パッカーへのコマンドである。パッカー・コマンドには、関連するBOMレコードを伴う部分のSCへの追加、BOMへのレコードの追加、および鍵記述部分へのレコードの追加が含まれる。
・上で説明したバッファに含まれる連結された構造体の数を示す値。
・BOM部分の名前と位置。
・各ビットが定義済みのフラグまたは将来の使用のための予約済みのフラグである値。現在、以下のフラグが定義されている。
ーバッファ内のすべての構造体を処理した後に、SCのすべての部分を一緒に単一のファイルにバンドルするかどうかに関する表示。部分の単一オブジェクトへのバンドルは、SCを作成する時に実行される最後のステップである。
ーディジタル署名をBOM部分から省略するかどうかに関する表示。このフラグがセットされていない場合には、SCを単一オブジェクトにバンドルする直前に、ディジタル署名が計算される。
【0139】代替実施形態では、SCを作成するためのパッカーへのインターフェースが、入力として下記のパラメータを受け入れるAPIによって行われる。
・まず、APIを呼び出して、SC BOM部分でIPレコードと表される、SC設定の初期設定に使用される情報、BOM部分に使用する名前、追加される部分を探すデフォルトの位置、およびフラグ値からなる構造体へのポインタを渡すことによって、材料表(BOM)部分を作成する。このAPIは、後続のパッカーAPIで使用されるSCハンドルを返す。
・パッカーは、部分をSCに追加する時に必ず使用されるAPIを有する。このAPIは、前のパッカーAPIによって返されたSCハンドル、追加される部分に関する情報からなる構造体へのポインタ、およびフラグ値を受け入れる。追加される部分に関する情報には、その部分の名前および位置、その部分についてBOM内で使用する名前、追加される部分のタイプ、その部分のハッシュ値、フラグなどが含まれる。
・すべての部分をSCに追加した後に、パッカーAPIを呼び出して、BOM部分を含むすべての部分を、通常はファイルである単一のSCオブジェクトにパックする。このAPIは、前のパッカーAPIによって返されたSCハンドル、パックされたSCに使用する名前、SCに署名するための情報を含む構造体へのポインタ、およびフラグ値を受け入れる。
【0140】パッカーまたはパッカーを呼び出す実体のいずれかは、SCテンプレートを使用してSCを作成することができる。SCテンプレートは、作成されるSC内で必要な部分およびレコードを定義する情報を有する。テンプレートでは、対称鍵623および暗号化される部分の暗号化に使用する暗号化方法および暗号化鍵の参照を定義することもできる。
【0141】パッカーは、SCのアンパックに使用されるAPIを有する。SCのアンパックは、SCをとり、個々の部分に分離する処理である。その後、パッカーを呼び出して、SCからアンパックされた暗号化された部分のいずれでも解読することができる。
【0142】B. 材料表(BOM)部分BOM部分は、SCが作成されつつある時にパッカーによって作成される。BOMは、SCに関する情報およびSCに含まれる部分に関する情報のレコードを含むテキスト・ファイルである。BOM内の各レコードは、単一の行にあり、改行が、新しいレコードの始まりを示す。BOMには、通常は、SCの認証性および保全性を検証するのに使用することができ

る、各部分のダイジェストと、ディジタル署名とが含まれる。BOM内のレコード・タイプは次の通りである。
【0143】IP IPレコードには、SCに関連する「名前＝値」対の組が含まれる。以下の名前が、SCの特定の特性のために予約されている。
V major.minor.fixV特性は、SCのバージョンを指定する。これは、SCがその下で作成されたSC仕様のバージョン番号である。Vに続く文字列は、major.minor.fixの形でなければならず、ここで、major、minor、およびfixは、それぞれメジャー・リリース番号、マイナー・リリース番号、および修正レベルである。
ID valueID特性は、このSCを作成しつつある実体によってこの特定のSCに割り当てられる一意の値である。valueのフォーマットは、この文書の後の版で定義される。
T valueT特性は、SCのタイプを指定する。タイプは次のいずれかでなければならない。
ORD － 注文SC650。
OFF － オファーSC641。
LIC － ライセンスSC。
TRA － トランザクションSC640。
MET － メタデータSC620。
CON － コンテンツSC630。
A valueA特性は、SCの著者または発行者を識別する。著者／発行者の識別は、曖昧でないか、クリアリングハウス105に登録されているか、その両方でなければならない。
D valueD特性は、SCが作成された日付と、任意選択で時刻を識別する。valueは、yyyy/mm/dd[@hh:mm[:ss[.fsec]][(TZ)]]の形でなければならず、これは、年／月／日@時：分：秒．10分の1秒（タイムゾーン）を表す。valueの任意選択部分は、[]文字で囲まれている。
E valueE 特性は、SCが満了する日付と、任意選択で時刻を識別する。valueは、前に定義したD特性に使用される形式と同一でなければならない。満了日付／時刻は、可能な時にはいつでも、クリアリングハウス105の日付／時刻と比較されなければならない。
CCURL valueCCURL特性は、クリアリングハウス105のURLを識別する。valueは、有効な外部URLの形式でなければならない。
H valueH特性は、SCに含まれる部分のメッセージ・ダイジェストの計算に使用されたアルゴリズムを識別する。ダイジェスト・アルゴリズムの例が、MD5である。
【0144】D Dレコードは、部分のタイプ、部分の名前、（任意選択の）部分のダイジェスト、および（任意選択の）部分がSCに含まれないことの表示を識別する情報を含む、データまたは部分エントリ・レコードである。タイプ識別子の直後の－記号は、その部分がSCに含まれないことを示すのに使用される。データまたは部分レコードの予約されているタイプは次の通りである。
K part_name [digest]鍵記述部分を指定する。
W part_name [digest]ウォーターマーキング命令部分を指定する。
C part_name [digest]ディジタル署名の検証に使用する証明書を指定する。
T part_name [digest]使用条件部分を指定する。
YF part_name [digest]オファーSC641のテンプレート部分を指定する。
YO part_name [digest]注文SC650のテンプレート部分を指定する。
YL part_name [digest]ライセンスSC660のテンプレート部分を指定する。
ID part_name [digest]参照されるコンテンツ113の項目のコンテンツ113のIDを指定する。
CH part_name [digest]クリアリングハウス105証明書部分を指定する。
SP part_name [digest]電子ディジタル・コンテンツ商店103証明書部分を指定する。
B part_name [digest]その部分または部分のサブセットがこのSCに含まれる別のSCのBOM部分を指定する。
BP part_name sc_part_name [digest]このSCに単一の部分として含まれる別のSCのBOM部分を指定する。sc_part_nameパラメータは、このSCに含まれ、このBOM部分が定義するSC部分の名前である。これと同一のBOMは、sc_part_nameパラメータによって定義されるSCにも含まれる。
D part_name [digest]データ（またはメタデータ）部分を指定する。
【0145】S Sレコードは、SCのディジタル署名の定義に使用される署名レコードである。ディジタル署名は、次のように指定される。
S key_identifier signature_string signature_algorithmSレコードには、署名の暗号化鍵を示すためのkey_identifier、ディジタル署名ビット列のbase64符号化であるsignature_string、およびディジタル署名を作成するためにダイジェストを暗号化するのに使用されたsignature_algorithmが含まれる。
【0146】C. 鍵記述部分鍵記述部分は、SCの暗号化された部分の解読に必要な暗号化鍵に関する情報を提供するために、パッカーによって作成される。暗号化された部分は、作成されるSCに含まれる場合があり、また、作成中のSCによって参照される他のSCに含まれる場合がある。鍵記述部分は、暗号化鍵と、その暗号化鍵が使用された部分に関する情報のレコードを含むテキスト・ファイルである。鍵記述部分の各レコードは、単一の行にあり、改行が、新しいレコードの始まりを示す。
【0147】以下のレコード・タイプが、鍵記述部分内で使用され、次のように定義されている。
【0148】
K encrypted_part_name; result_part_name; part_encryption_algorithm_identifier; public_key_identifier key_encryption_algorithmおよびencrypted_symmetric_key【0149】Kレコードは、このSCに含まれる可能性があるか、このレコードによって参照される別のSCに含まれる可能性がある暗号化された部分を指定する。encrypted_part_nameは、このSCの部分の名前または、別のSC内の暗号化された部分の名前を指すURLのいずれかである。result_part_nameは、解読された部分に与えられる名前である。
part_encryption_algorithm_identifierは、その部分の暗号化に使用された暗号化アルゴリズムを示す。public_key_identifierは、対称鍵623の暗号化に使用された鍵の識別子である。
【0150】key_encryption_algorithm_identifierは、対称鍵623の暗号化に使用された暗号化アルゴリズムを示す。
encrypted_symmetric_keyは、その部分の暗号化に使用された暗号化された対称鍵623のビット列のbase64符号化である。
【0151】VII. クリアリングハウス105A. 概要クリアリングハウス105は、セキュア・ディジタル・コンテンツ電子配布システム100の権利管理機能の責任を負う。クリアリングハウス105の機能には、電子ディジタル・コンテンツ商店103の使用可能化、コンテンツ113の権利の検証、購入トランザクションおよび関連情報の保全性および認証性の検証、エンドユーザ装置109へのコンテンツ暗号化鍵または対称鍵623の配布、これらの鍵の配布の追跡、および電子ディジタル・コンテンツ商店103およびコンテンツ・プロバイダ101へのトランザクション要約の報告が含まれる。コンテンツ暗号化鍵は、通常は認証電子ディジタル・コンテンツ商店103からの購入トランザクションによって、権利を取得したコンテンツ113のロックを解除するために、エンドユーザ装置109によって使用される。コンテンツ暗号化鍵をエンドユーザ装置109に送信する前に、クリアリングハウス105は、検証処理をすべて実行して、コンテンツ113を売る実体の認証性と、コンテンツ113に対してエンドユーザ装置109が有する権利を検証する。これを、SC分析

ツール185と呼ぶ。いくつかの構成では、クリアリングハウス105は、クレジット・カード認証および請求という電子ディジタル・コンテンツ商店103の機能を実行するシステムをクリアリングハウス105で同じ場所に配置することによって、コンテンツ113購入の会計清算を処理することもできる。クリアリングハウス105は、ICVerifyおよびTaxwareなどのOEMパッケージを使用して、クレジット・カード処理およびローカル売上税を処理する。

【0152】電子ディジタル・コンテンツ商店の実施形態セキュア・ディジタル・コンテンツ電子配布システム100内にコンテンツ113の売り手として参加したい電子ディジタル・コンテンツ商店103は、コンテンツ113をセキュア・ディジタル・コンテンツ電子配布システム100に供給する1つまたは複数のディジタル・コンテンツ・プロバイダ101に要求を行う。2つの当事者が合意に達する限り、要求を行うための決定的な処理はない。たとえばSony、Time-Warnerなどの音楽レーベルなどのディジタル・コンテンツ・レーベルが、電子ディジタル・コンテンツ商店103にそのコンテンツ113を販売することを許可すると決定した後に、クリアリングハウス105が、通常は電子メールを介して、電子ディジタル・コンテンツ商店103をセキュア・ディジタル・コンテンツ電子配布システム100に追加する要求について連絡を受ける。ディジタル・コンテンツ・レーベルは、電子ディジタル・コンテンツ商店103の名前と、電子ディジタル・コンテンツ商店103のディジタル証明書を作成するためにクリアリングハウス105が必要とする可能性がある他のすべての情報を供給する。このディジタル証明書は、保護された形でディジタル・コンテンツ・レーベルに送信され、その後、ディジタル・コンテンツ・レーベルによって、電子ディジタル・コンテンツ商店103に転送される。クリアリングハウス105は、それが割り当てたディジタル証明書のデータベースを維持する。各証明書には、バージョン番号、一意の通し番号、署名アルゴリズム、発行者の名前(たとえばクリアリングハウス105の名前)、その証明書が有効とみなされる日付の範囲、電子ディジタル・コンテンツ商店103の名前、電子ディジタル・コンテンツ商店103の公開鍵、およびクリアリングハウス105の秘密鍵を使用して署名された他の情報のすべてのハッシュ・コードが含まれる。クリアリングハウス105の公開鍵621を有する実体は、証明書を検証することができ、その後、証明書からの公開鍵を使用して検証できる署名を有するSCが有効なSCであることを確認することができる。

【0153】電子ディジタル・コンテンツ商店103は、クリアリングハウス105によって作成されたそのディジタル証明書およびディジタル・コンテンツ・レーベルからのSCを処理するのに必要なツールを受信した後に、エンドユーザが購入することのできるコンテンツ113の提供を始めることができる。電子ディジタル・コンテンツ商店103には、その証明書とトランザクションSC640が含まれ、電子ディジタル・コンテンツ商店103は、そのディジタル署名643を使用してSCに署名する。エンドユーザ装置109は、まず、ディジタル証明書取消リストを検査し、次に、クリアリングハウス105の公開鍵621を使用して電子ディジタル・コンテンツ商店103のディジタル証明書の情報を検証することによって、電子ディジタル・コンテンツ商店103がセキュア・ディジタル・コンテンツ電子配布システム100上のコンテンツ113の有効なディストリビュータであることを検証する。ディジタル証明書取消リストは、クリアリングハウス105によって維持される。取消リストは、クリアリングハウス105によって作成されるライセンスSC660に、部分の1つとして含めることができる。エンドユーザ装置109は、エンドユーザ装置109上で取消リストのコピーを保持し、したがって、これを電子ディジタル・コンテンツ商店103のディジタル証明書検証の一部として使用することができる。エンドユーザ装置109は、ライセンスSC660を受信した時に、必ず、新しい取消リストが含まれているかどうかを判定し、そうである場合には、エンドユーザ装置109上のローカル取消リストを更新する。

【0154】B. 権利管理処理注文SCの分析クリアリングハウス105は、エンドユーザが電子ディジタル・コンテンツ商店103からオファーSC641を含むトランザクションSC640を受信した後に、エンドユーザからの注文SC650を受信する。注文SC650は、コンテンツ113およびその使用に関連する情報、コンテンツ113を販売しようとしている電子ディジタル・コンテンツ商店103に関する情報、および、コンテンツ113を購入しようとしているエンドユーザに関する情報を含む部分からなる。クリアリングハウス105は、注文SC650の情報の処理を開始する前に、まず、そのSCが実際に有効であり、それに含まれるデータがどのような形でも壊れていないことを確実にするために、いくつかの処理を実行する。

【0155】検証クリアリングハウス105は、ディジタル署名を検証することによって注文SC650の検証を開始し、その後、クリアリングハウス105は、注文SC650の諸部分の保全性を検証する。ディジタル署名を検証するために、まず、クリアリングハウス105は、署名付きの場合に含まれる署名する実体の公開鍵661を使用して、署名自体のコンテンツ631を解読する(署名する実体は、コンテンツ・プロバイダ101、電子ディジタル・コンテンツ商店103、エンドユーザ装置109、またはこれらの組合せとすることができる)。その後、クリアリングハウス105は、SCの連結された部分ダイジェストのダイジェストを計算し、ディジタル署名の暗号化されたコンテンツ113と比較する。2つの値が一致する場合には、ディジタル署名が有効である。各部分の保全性を検証するために、クリアリングハウス105は、その部分のダイジェストを計算し、BOM内のダイジェスト値と比較する。クリアリングハウス105は、同一の処理に従って、注文SC650内に含まれるメタデータおよびオファーSC641の部分のディジタル署名および部分の保全性を検証する。

【0156】トランザクションSC640およびオファーSC641のディジタル署名の検証の処理では、電子ディジタル・コンテンツ商店103がセキュア・ディジタル・コンテンツ電子配布システム100によって許可されていることも、間接的に検証される。これは、クリアリングハウス105が、証明書の発行者であるという事実に基づく。その代わりに、クリアリングハウス105が、電子ディジタル・コンテンツ商店103からの公開鍵を使用してトランザクションSC640およびオファーSC641のディジタル署名を成功裡に検証することができるが、これは、SCに署名する実体が関連する秘密鍵の所有権を有する場合に限られる。電子ディジタル・コンテンツ商店103だけが、秘密鍵の所有権を有する。クリアリングハウス105が、電子ディジタル・コンテンツ商店103のローカル・データベースを有する必要がないことに留意されたい。というのは、商店が、クリアリングハウスの公開鍵を使用してトランザクションSC640のオファーSC641の公開鍵に署名するからである。

【0157】その後、エンドユーザが購入しようとしているコンテンツ113の商店使用条件519が、クリアリングハウス105によって検証されて、この商店使用条件519がメタデータSC620で設定された制約の中に含まれることを確実にする。メタデータSC620は、注文SC650内に含まれることを想起されたい。

【0158】鍵の処理暗号化された対称鍵623およびウォーターマーキング命令の処理は、注文SC650の認証性および保全性の検査、電子ディジタル・コンテンツ商店103の検証、および商店使用条件519の検証が成功裡に完了した後に、クリアリングハウス105によって行われる。注文SC650のメタデータSC620部分は、通常は、クリアリングハウス105の公開鍵621を使用して暗号化された複数の対称鍵623を、鍵記述部分に配置されている。対称鍵623の暗号化は、メタデータSC620の作成時にコンテンツ・プロバイダ101によって行われる。

【0159】1つの対称鍵623が、ウォーターマーキング命令の解読に使用され、他の対称鍵は、コンテンツ113および暗号化されたメタデータの解読に使用される。コンテンツ113は、単一の曲またはCDの曲の集号全体を表すことができるので、曲ごとに異なる対称鍵623を使用することができる。ウォーターマーキング命令は、注文SC650のメタデータSC620部分に含まれる。コンテンツ113および暗号化されたメタデータは、コンテンツ・ホスティング・サイト111のコンテンツSC630内にある。コンテンツSC630内の暗号化されたコンテンツ113部分およびメタデータ部分のURLおよび部分名は、注文SC650のメタデータSC620部分の鍵記述部分に含まれる。クリアリングハウス105は、その秘密鍵を使用して、対称鍵623を解読し、その後、これらのそれぞれを、エンドユーザ装置109の公開鍵661を使用して暗号化する。エンドユーザ装置109の公開鍵661は、注文SC650から取り出される。新たに暗号化された対称鍵623は、クリアリングハウス105がエンドユーザ装置109に返すライセンスSC660の鍵記述部分に含まれる。

【0160】対称鍵623の処理の時間の間に、クリアリングハウス105が、ウォーターマーキング命令に対する変更を行いたくなる場

合がある。その場合には、クリアリングハウス105が対称鍵623を解読した後に、ウォーターマーキング命令が変更され、再暗号化される。新しいウォーターマーキング命令は、エンドユーザ装置109に返されるライセンスSC660内の部分の1つとして含まれる。
【0161】注文SC650の処理のすべてに成功した場合、クリアリングハウス105は、ライセンスSC660をエンドユーザ装置109に返す。エンドユーザ装置109は、ライセンスSC660の情報を使用して、コンテンツSC630をダウンロードし、暗号化されたコンテンツ113およびメタデータにアクセスする。ウォーターマーキング命令も、エンドユーザ装置109によって実行される。
【0162】クリアリングハウス105が、注文SC650を成功裡に処理することができない場合には、HTMLページがエンドユーザ装置109に返され、インターネット・ブラウザ・ウィンドウに表示される。このHTMLページには、クリアリングハウス105がトランザクションを処理できなかった理由が示される。
【0163】代替実施形態では、ユーザが、販売について設定された公開日付の前にコンテンツ113のコピーを購入した場合に、ライセンスSC660が、対称鍵623なしで返される。ライセンスSC660は、公開日またはその後に、対称鍵623を受け取るためにクリアリングハウス105に返される。一例として、コンテンツ・プロバイダ101は、新曲の公開日の前にユーザがその曲をダウンロードできるようにして、コンテンツ・プロバイダ101によって設定された日付の前に顧客がその曲をダウンロードし、その曲を再生する準備を行えるようにする。これによって、公開日の帯域幅およびダウンロード時間に関する競争なしで、公開日にコンテンツ113を即座にオープンすることができるようになる。
【0164】C. 国固有のパラメータ任意選択として、クリアリングハウス105は、エンドユーザ装置109のドメイン・ネームと、可能な時には必ずクレジット・カード請求先住所を使用して、エンドユーザの国位置を判定する。エンドユーザが居住する国でコンテンツ113の販売に関する制限がある場合には、クリアリングハウス105は、ライセンスSC660をエンドユーザ装置109に送信する前に、処理中のトランザクションがこれらの制限に違反しないことを保証する。電子ディジタル・コンテンツ商店103も、クリアリングハウス105と同一の検査を実行することによって、さまざまな国へのコンテンツ113の配布の管理に参加することが期待される。クリアリングハウス105は、電子ディジタル・コンテンツ商店103が、コンテンツ・プロバイダ101によって設定された国固有の規則を無視している場合には、可能なすべての検査を行う。
【0165】D. 監査ログおよび追跡クリアリングハウス105は、コンテンツ113購入トランザクション中および報告要求トランザクション中に実行される動作ごとの情報の監査ログ150を維持する。この情報は、セキュア・ディジタル・コンテンツ電子配布システム100の監査、報告の生成、およびデータ・マイニングなどのさまざまな目的に使用することができる。
【0166】クリアリングハウス105は、電子ディジタル・コンテンツ商店103の請求サブシステム182の残高勘定も維持する。電子ディジタル・コンテンツ商店103の価格決定構造が、ディジタル・コンテンツ・レーベルによってクリアリングハウス105に供給される。この情報には、現在の特価、数量割引、および電子ディジタル・コンテンツ商店103に課す必要がある勘定赤字限度などを含めることができる。クリアリングハウス105は、価格決定情報を使用して、電子ディジタル・コンテンツ商店103の残高を追跡し、電子ディジタル・コンテンツ商店103がコンテンツ・プロバイダ101によって設定された赤字限度を超えないことを保証する。
【0167】以下の動作は、通常はクリアリングハウス105によってログ記録される。
・ライセンスSC660を求めるエンドユーザ装置109の要求・クリアリングハウス105が請求を処理する時のクレジット・カード認証番号
・エンドユーザ装置109へのライセンスSC660の分散・報告の要求・コンテンツSC630およびライセンスSC660が受信され、検証されたことのエンドユーザからの通知【0168】以下の情報は、通常は、ライセンスSC660に関してクリアリングハウス105によってログ記録される。
・要求の日付および時刻・購入トランザクションの日付および時刻・購入される項目のコンテンツID・コンテンツ・プロバイダ101の識別・商店使用条件519・ウォーターマーキング命令の変更・電子ディジタル・コンテンツ商店103によって追加されたトランザクションID535・電子ディジタル・コンテンツ商店103の識別・エンドユーザ装置109の識別・エンドユーザのクレジット・カード情報（クリアリングハウス105が請求を処理する場合）
【0169】以下の情報は、通常は、エンドユーザのクレジット・カード検証のためにクリアリングハウス105によってログ記録される。
・要求の日付および時刻・クレジット・カードに請求される金額・購入される項目のコンテンツID・電子ディジタル・コンテンツ商店103によって追加されたトランザクションID535・電子ディジタル・コンテンツ商店103の識別・エンドユーザの識別・エンドユーザのクレジット・カード情報・クレジット・カードの清算者から受け取った許可番号
【0170】以下の情報は、通常は、ライセンスSC660がエンドユーザ装置109に送信される時にクリアリングハウス105によってログ記録される。
・要求の日付および時刻・購入される項目のコンテンツID・コンテンツ・プロバイダ101の識別・使用条件517・電子ディジタル・コンテンツ商店103によって追加されたトランザクションID535・電子ディジタル・コンテンツ商店103の識別・エンドユーザの識別【0171】以下の情報は、通常は、報告要求が行われた時にログ記録される。
・要求の日付および時刻・報告書発送の日付および時刻・要求された報告のタイプ・報告を生成するのに使用したパラメータ・報告を要求した実体の識別子【0172】E. 結果の報告報告は、エンドユーザ購入トランザクション中にクリアリングハウス105がログ記録した情報を使用して、クリアリングハウス105によって生成される。コンテンツ・プロバイダ101および電子ディジタル・コンテンツ商店103は、支払検証インターフェース183を介してクリアリングハウス105にトランザクション報告を要求することができ、したがって、これらは、これら自体のトランザクション・データベースをクリアリングハウス105によってログ記録された情報と一致させることができる。クリアリングハウス105は、コンテンツ・プロバイダ101および電子ディジタル・コンテンツ商店103に定期的な報告を供給することもできる。
【0173】クリアリングハウス105は、コンテンツ・プロバイダ101および電子ディジタル・コンテンツ商店103が報告を要求でき、報告を受信できるようにするセキュア電子インターフェースを定義する。報告要求SCには、要求を開始する実体にクリアリングハウス105によって割り当てられた証明書が含まれる。クリアリングハウス105は、この証明書とSCのディジタル署名を使用して、その要求が許可された実体から発したことを検証する。要求には、持続時間など、報告の範囲を定義するパラメータも含まれる。クリアリングハウス105は、要求パラメータを検証して、要求元が、有することを許可される情報だけを受け取ることができるようにする。
【0174】クリアリングハウス105が、報告要求SCが真正であり有効であると判定した場合、クリアリングハウス105は、報告を生成し、報告SCにパックして、要求を開始した実体に送信する。いくつかの報告を、定義済みの時間間隔で自動的に生成し、クリアリングハウス105に格納して、要求を受信した時に即座に送信できるようにすることができる。報告に含まれるデータのフォーマットは、この文書の後の版で定義される。
【0175】F. 請求および支払の検証コンテンツ113の請求は、クリアリングハウス105または電子ディジタル・コンテンツ商店103のいずれかが処理することができる。クリアリングハウス105が電子的なコンテンツ113の請求を処理する場合には、電子ディジタル・コンテンツ商店103は、エンドユーザの注文を、電子商品と、適用可能であれば物理的商品に分離する。電子ディジタル・コンテンツ商店103は、エンドユーザの請求情報および許可される必要がある合計額を含むトランザクションについてクリアリングハウス105に通知する。クリアリングハウス105は、エンドユーザのクレジット・カードを許可し、電子ディジタル・コンテンツ商店103に通知を返す。クリアリングハウス105が、エンドユーザのクレジット・カードを許可するのと同時に、電子ディジタル・コンテンツ商

店103は、購入される物理的商品についてエンドユーザのクレジット・カードに請求することができる。各電子項目がエンドユーザ装置109によってダウンロードされた後に、クリアリングハウス105が通知を受け、したがって、エンドユーザのクレジット・カードに請求することができる。これは、コンテンツ113がエンドユーザ装置109での使用を可能にされる前に、エンドユーザ装置109によって最後のステップとして行われる。

【0176】電子ディジタル・コンテンツ商店103が電子的なコンテンツ113の請求を処理する場合、クリアリングハウス105は、エンドユーザ装置109がクリアリングハウス105に注文SC650を送信するまで、トランザクションについて通知されない。しかし、クリアリングハウス105は、各電子項目がダウンロードされた後に、エンドユーザ装置109によって通知される。クリアリングハウス105は、通知された時に、電子ディジタル・コンテンツ商店103に通知を送信し、その結果、電子ディジタル・コンテンツ商店103は、エンドユーザのクレジット・カードに請求することができる。

【0177】G. 再送信セキュア・ディジタル・コンテンツ電子配布システム100は、コンテンツ113の再送信を処理する能力を提供する。これは、通常は、顧客サービス・インターフェース184によって実行される。電子ディジタル・コンテンツ商店103は、再送信を開始するためにエンドユーザが1ステップずつ進むことのできるユーザ・インターフェースを提供する。エンドユーザは、コンテンツ113の再送信を要求するために、コンテンツ113項目を購入した電子ディジタル・コンテンツ商店103のサイトに行く。

【0178】コンテンツ113の再送信は、コンテンツ113をダウンロードできなかったかダウンロードしたコンテンツ113が使用不能なので、エンドユーザが前に購入したコンテンツ113の新しいコピーを要求する時に行われる。電子ディジタル・コンテンツ商店103は、エンドユーザがコンテンツ113の再送信を行う資格を有するかどうかを判定する。エンドユーザが再送信の資格を有する場合には、電子ディジタル・コンテンツ商店103は、再送信されるコンテンツ113項目のオファーSC641を含むトランザクションSC640を作成する。このトランザクションSC640が、エンドユーザ装置109に送信され、購入トランザクションと同一のステップが、エンドユーザによって実行される。エンドユーザ装置109が、再送信が進行中のコンテンツ113項目の鍵ライブラリ内にスクランブル化された鍵を有する場合には、トランザクションSC640に、エンドユーザ装置109がスクランブル化された鍵を削除するように指示する情報が含まれる。

【0179】クリアリングハウス105が、コンテンツ113購入の会計清算を処理する場合には、電子ディジタル・コンテンツ商店103は、トランザクションSC640内に、注文SC650内でクリアリングハウス105に運ばれるフラグを含める。クリアリングハウス105は、注文SC650のフラグを解釈し、コンテンツ113の購入についてエンドユーザに請求せずにトランザクションを進める。

【0180】VIII. コンテンツ・プロバイダA. 概要セキュア・ディジタル・コンテンツ電子配布システム100のコンテンツ・プロバイダ101は、ディジタル・コンテンツ・レーベルであるか、コンテンツ113に対する権利を所有する実体である。コンテンツ・プロバイダ101の役割は、配布のためにコンテンツ113を準備し、コンテンツ113に関する情報を、電子ディジタル・コンテンツ商店103またはコンテンツ113のダウンロード可能電子版の小売業者に使用可能にすることである。最高のセキュリティおよび権利制御をコンテンツ・プロバイダ101に提供するために、一連のツールを設けて、コンテンツ・プロバイダ101がその構内でそのコンテンツ113を準備し、SCに安全にパッケージ化できるようにし、その結果、コンテンツ113が、コンテンツ・プロバイダ101のドメインを離れる時に保護され、絶対に露出されず、許可されない当事者によってアクセス可能にならないようにする。これによって、コンテンツ113を、インターネットなどの保護されないネットワークを介して、ハッカーまたは許可されない当事者への露出の恐れなしに、自由に配布できるようになる。

【0181】コンテンツ・プロバイダ101用のツールの最終目的は、曲または一連の曲などのコンテンツの113を準備し、コンテンツSC630にパッケージ化し、曲を記述した情報、曲の承認される使用(コンテンツの使用条件517)、および曲の販売促進情報をメタデータSC620にパッケージ化することである。これを達成するために、以下のツールのセットを提供する。

・ワーク・フロー・マネージャ154 処理活動をスケジューリングし、処理の必要な同期化を管理する。

・コンテンツ処理ツール155 ウォーターマーキング、前処理(オーディオの例の場合、必要な等化、動的特性調整、または再サンプリング)符号化および圧縮を含む、コンテンツ113ファイル準備を制御するためのツールの集合。

・メタデータ同化および入力ツール161 コンテンツ・プロバイダのデータベース160またはサード・パーティ・データベースまたはデータ・インポート・ファイルまたは操作員介入を介してコンテンツ113記述情報を収集し、コンテンツの使用条件517を指定する手段を提供するのに使用されるツールの集合。CDSファイルまたはDDPファイル用のディジタル・オーディオ・コンテンツなどのコンテンツをキャプチャまたは抽出するためのインターフェースも設けられる。品質管理ツールが、準備されたコンテンツおよびメタデータのプレビューを可能にする。メタデータに対して必要な訂正またはさらに処理するためのコンテンツの再サブミットを行うことができる。

・SCパッカー・ツール152 コンテンツ113および情報のすべてを暗号化し、パッケージ化し、SCパッカーを呼び出してSCにパックする。

・コンテンツ分散ツール(図示せず) コンテンツ・ホスティング・サイト111および電子ディジタル・コンテンツ商店103などの指定された配布センタにSCを分散する。

・コンテンツ販売促進ウェブ・サイト156 許可された電子ディジタル・コンテンツ商店103によるダウンロードのためのメタデータSC620と、任意選択として追加の販売促進材料を記憶する。

【0182】B. ワーク・フロー・マネージャ154このツールの目的は、コンテンツ113の処理活動のスケジューリング、追跡、および管理である。このアプリケーションによって、マルチユーザ・アクセスが可能になり、コンテンツ・プロバイダ101のイントラネットまたはエクストラネット内の遠隔位置からのコンテンツ113のスケジューリングおよび状況検査が可能になる。この設計では、複数の個人がコンテンツ113の複数の部分を並列に操作することができ、異なる個人に特定の責任を割り当てることができ、これらの個人が全世界に散在することができる、コラボレーション処理も可能になる。

【0183】図11に移ると、この図は、図10に対応するワーク・フロー・マネージャ154の主要な処理のブロック図である。図11の主要な処理に、この節で説明するツールによって提供されるコンテンツ113処理機能が要約されている。ワーク・フロー・マネージャ154は、これらの処理にジョブを供給し、現在の処理の完了時にジョブを次に必要な処理に向ける責任を負う。これは、下記の目的のために各処理ツールが呼び出す一連のアプリケーション・プログラミング・インターフェース(API)を介して達成される。

・次に処理するジョブを取り出す・処理の成功裡の完了を示す・処理の不成功の完了と失敗の理由を示す・処理の中間状況を供給する(依存処理の部分的な完了だけを必要とする処理を開始できるようにするため)

・指定された処理から使用可能にされる製品にコメントを追加する【0184】ワーク・フロー・マネージャ154は、ユーザ・インターフェースも有し、ワーク・フロー・マネージャ・ユーザ・インターフェース700の一例が、図10に示されており、これは、以下の機能を提供する。

・処理のさまざまな段階で割り当てられ、実行されるデフォルト値およびデフォルト条件の指定を可能にする構成パネル・ワーク・フロー・ルールおよび自動化処理フローのカスタマイズ・ジョブ・スケジューリング・状況の照会および報告・1つまたは複数の処理に関連するジョブに関するコメントまたは命令の追加・ジョブ管理(すなわち、中断、解放、除去、優先順位(処理の順序)変更)

【0185】各処理は、ワーク・フロー・マネージャ154によって管理されるキューを関連付けられる。ワーク・フロー・マネージャ154にジョブを要求するすべての処理が、ワーク・フロー・マネージャによる、現在それに関連するキューにジョブがない場合にはその処理(ツール)の待機状態での中断、またはめいめいの処理の実行に必要なジョブに関するすべての情報を処理に返すことをもたらす。ある処理が待機状態で中断されている場合に、その処理は、ジョブがワーク・フロー・マネージャ154によってそのキューに

配置された時に処理を再開する。
【0186】ワーク・フロー・マネージャ154は、定義済みのルールの組に基づいて、処理のフローまたは順序も管理する。これらのルールは、コンテンツ・プロバイダ101が、特別な処理要件を有するか、固有のデフォルト・ルールを構成する場合に、コンテンツ・プロバイダ101がカスタマイズすることができる。ある処理が、それに割り当てられたタスクの完了を報告する時には、その処理は、この状況についてワーク・フロー・マネージャ154に通知し、ワーク・フロー・マネージャ154は、定義済みのルールに基づいて、そのジョブが次に配置されるキューを決定する。
【0187】特殊な処理命令または通知を示すコメントを、プログラミングAPIを介するか、ワーク・フロー・マネージャ・ユーザ・インターフェース700またはプロセッサ・インターフェースを介して手動でのいずれかで、処理ステップのいずれかで製品に添付することもできる。
【0188】ワーク・フロー・マネージャ154の処理は、好ましい実施形態ではJavaで実施されるが、C／C＋＋、アセンブラ、および同等物などの他のプログラミング言語を使用することができる。ワーク・フロー・マネージャ154に関して下で説明する処理は、さまざまなハードウェア・プラットホームおよびソフトウェア・プラットホーム上で稼動することができることを理解されたい。完全なシステムとしてのまたはそれを構成する処理のいずれかとしてのワーク・フロー・マネージャ154は、ウェブなどの電子配布、またはフロッピ・ディスケット、CD－ROM、および取外し可能ハード・ディスク装置を含むがこれらに制限されないコンピュータ可読媒体内のアプリケーション・プログラムとして配布することができる。
【0189】ここで図11に移ると、この図は、図10に対応するワーク・フロー・マネージャ154の主要な処理のブロック図である。以下の節では、各処理を要約し、各処理に必要な情報または処置を説明する。
【0190】1. 処置／情報待機中製品処理801ジョブが特定の処理キューに配置されるのは、その処理が必要とするすべての情報が使用可能になり、そのジョブがすべての依存処理を成功裡に完了した後である。ワーク・フロー・マネージャ154には、欠けている情報または次の処理を妨げる失敗に起因して処理のために現在使用可能ではないジョブを保持するのに使用される特殊なキューが存在する。これらのジョブは、処置／情報待機中製品処理801キューに配置される。このキューの各ジョブは、それが待っている処置または情報、このジョブを最後に操作した処理、および欠けている情報または追加情報が供給されるか必要な処置が成功裡に完了した後にこのジョブがキューに入れられる次の処理を示すための関連する状況を有する。
【0191】処理の完了は、ワーク・フロー・マネージャ154による、このキューの検査と、このキューのジョブがこの処理（処置）の完了またはこの処理によって供給される情報を待っているかどうかの判定を引き起こす。そうである場合には、そのジョブは、適当な処理キューに入れられる。
【0192】2. 新規コンテンツ要求処理802コンテンツ・プロバイダ101は、電子的に販売し、配布したい製品（たとえば、製品は、曲または曲の集合とすることができる）を決定する。ワーク・フロー・マネージャ154の初期機能は、操作員が、これらの製品を識別でき、新規コンテンツ要求処理802のキューに配置できるようにすることである。コンテンツ・プロバイダ101は、構成オプションを介して、製品選択インターフェース上でどの情報についてプロンプトを表示するかを指定することができる。製品を一意に識別するのに十分な情報が入力される。任意選択として、追加フィールドを含めて、メタデータ獲得と並列にオーディオ処理相を開始するのに必要な情報の手入力を要求することができる。手動で供給されない場合には、この情報を、任意選択として、デフォルト構成設定から、または、自動メタデータ獲得処理803でメタデータ処理の第1段階で得られるコンテンツ・プロバイダのデータベース160から、取り出すことができる。コンテンツ・プロバイダのデータベース160でのコンテンツ113の構造および機能によって、コンテンツ選択処理が決定される。
【0193】コンテンツ・プロバイダ101のデータベース160への照会を実行するのに必要な、要求される情報が指定される場合、ジョブは、自動メタデータ獲得処理803によって処理される。音楽の実施形態では、オーディオ処理のために製品を正しくスケジューリングするために、製品のジャンルおよび所望の圧縮レベルならびにオーディオPCMファイル名またはオーディオWAVファイル名が、指定される。この情報は、製品選択処理の一部として入力するか、カスタマイズされた照会インターフェースまたはウェブ・ブラウザ機能を介して選択することができる。この情報を指定することによって、コンテンツ処理のために製品をスケジューリングできるようになる。
【0194】製品選択ユーザ・インターフェースは、製品を処理のために公開するかどうか、または、さらに情報を入力するために保留状態に保持するかどうかを操作員が指定できるようにするオプションを提供する。保持される場合、ジョブは、新規コンテンツ要求処理802のキューに追加され、データ入力の完了または処理のための製品の公開のために次の処置を待つ。製品が公開された後に、ワーク・フロー・マネージャ154は、指定された情報を評価し、そのジョブがどの処理に渡される準備ができているかを判定する。
【0195】コンテンツ・プロバイダ101のデータベース160への自動化された照会を可能にするのに適当な情報が供給される場合、ジョブは、自動メタデータ獲得処理803のキューに入れられる。データベース・マッピング・テーブルが、自動メタデータ獲得処理803のために構成されていない場合には、ジョブは、手動メタデータ入力処理804のキューに入れられる（データベース・マッピング・テーブルの詳細については、自動メタデータ獲得処理803の節を参照されたい）。
【0196】オーディオ処理に必要な一般情報およびウォーターマーキングに必要な特定の情報が指定された場合、ジョブは、ウォーターマーキング処理808（コンテンツ処理の最初の相）のキューに入れられる。ジョブが解放された時に必要な情報のいずれかが欠けている場合、そのジョブは、欠けている情報を示す状況と共に、処置／情報待機中製品処理801のキューに入れられる。
【0197】状況から、コンテンツ113のファイル名、たとえばコンテンツ113がオーディオの場合にPCMファイルまたはWAVファイルの名前が欠けていることが示される場合、これが、キャプチャ（またはディジタル媒体からのディジタル抽出）が必要であることを示す場合がある。オーディオ処理機能は、曲ファイルが標準ファイル・システム・インターフェースを介してアクセス可能であることを必要とする。曲が、外部媒体または、オーディオ処理ツールから直接アクセス可能でないファイル・システムに配置されている場合には、そのファイルを、まずアクセス可能なファイル・システムにコピーする。曲が、ディジタル形式であるがCDまたはディジタル・テープ上にある場合には、それらの曲を、オーディオ処理ツールからアクセス可能なファイル・システムに抽出する。ファイルがアクセス可能になった後に、ワーク・フロー・マネージャ・ユーザ・インターフェース700を使用して、ジョブに関するパスおよびファイル名を指定または選択し、その結果、ウォーターマーキングに必要な他のすべての情報も指定されたと仮定して、そのジョブをウォーターマーキング処理に公開可能にすることができる。
【0198】3. 自動メタデータ獲得処理803自動メタデータ獲得処理803は、コンテンツ・プロバイダ101のデータベース160またはデータがインポートされている場合にはステージング・データベースに対する一連の照会を実行して、自動化された形でできる限り多くの製品情報を得ることを試みる。自動メタデータ獲得処理803は、項目をそのキューに配置することが可能になる前に、以下の情報を必要とする。
・コンテンツ・プロバイダ101のデータベース160への照会を生成するのに適当な情報を有するデータベース・マッピング・テーブル・照会を実行するのに必要な製品情報・製品を一意に定義するのに適当な製品情報【0199】コンテンツ・プロバイダ101のデータベース160への自動化された照会を実行して、このコンテンツ113を処理するのに必要な情報を得る。たとえば、コンテンツ113が音楽の場合、この照会を実行するのに必要な情報は、アルバム名であるか、UPC（統一商品コード）またはコンテンツ・プロバイダ101によって定義される特定のアルバムIDまたは選択IDである可能性がある。得られる情報のうちで、一部が必要として指定される（詳細については自動メタデータ獲得処理803の節を参照されたい）。必要な情報のすべてが得られた場合、ジョブは、次

に、使用条件処理805のキューに入れられる。必要な情報のどれかが欠けている場合には、曲は、手動メタデータ入力処理804のキューに入れられる。処置／情報待機中製品処理801のキューのジョブのどれかが、このステップで得られる情報のどれかを待っている場合には、そのジョブの状況を更新して、もはやこの情報を待っていないことを示す。そのジョブがもはや未解決の必要条件を有しない場合には、そのジョブは、次に定義されたキューに入れられる。

【0200】4. 手動メタデータ入力処理804手動メタデータ入力処理804は、操作員が欠けている情報を入力する手段を提供する。手動メタデータ入力処理804は、依存性を有しない。すべての必要な情報が指定された後に、ジョブは、使用条件処理805のキューに入れられる。

【0201】5. 使用条件処理805使用条件処理805では、製品の使用および制限を指定することができる。使用条件処理805は、いくつかのメタデータを必要とする場合がある。使用条件指定の完了時に、ジョブは、監視公開処理806オプションが要求されたか、監視公開処理806オプションがワーク・フロー・マネージャ154のルールでデフォルトとして構成される場合を除いて、メタデータSC作成処理807のキューに入れられる資格を有する。上記の場合には、ジョブは、監視公開処理806のキューに入れられる。メタデータSC作成処理807のキューに入れる前に、ワーク・フロー・マネージャ154は、まず、その処理のすべての依存性が満たされている（下を参照されたい）ことを確認する。そうでない場合には、ジョブは、処置／情報待機中製品処理801のキューに入れられる。

【0202】6. 監視公開処理806監視公開処理806では、品質検査と、ディジタル・コンテンツ製品について指定される情報の検証を行うことができる。監視公開処理806は、依存性を有しない。前にこの製品について処理の段階でジョブに付加されたコメントを、スーパーバイザが再検討し、適当な処置を講ずることができる。すべての情報およびコメントを再検討した後に、スーパーバイザは、以下の選択肢を有する。

・公開を承認し、製品をメタデータSC作成処理807のキューに入れる・情報の変更または追加を行い、製品をメタデータSC作成処理807のキューに入れる・ジョブにコメントを追加し、もう一度手動メタデータ入力処理804のキューに入れる・コメントを追加し、ジョブを処置／情報待機中製品処理801のキューに入れる【0203】7. メタデータSC作成処理807メタデータSC作成処理807は、上で収集された情報ならびにメタデータSC620に必要な他の情報のすべてを一緒に集め、SCパッカー処理を呼び出して、メタデータSC620を作成する。このツールは、入力として下記を必要とする。

・必要なメタデータ・使用条件・この製品のすべての品質レベルの暗号化段階で使用される暗号化鍵【0204】この最後の依存性は、メタデータSC620を作成する前に、関連するオーディオ・オブジェクトが、オーディオ処理相を完了することを必要とする。メタデータSC作成処理807の完了時に、ジョブは、定義済みのワーク・フロー・ルールに基づいて、最終品質保証処理813またはコンテンツ分散処理814のいずれかのキューに入れられる。

【0205】8. ウォーターマーキング処理808ウォーターマーキング処理808は、コンテンツ113に著作権情報および他の情報を追加する。コンテンツ113が音楽である実施形態の場合、このツールは、入力として下記を必要とする。

・曲のファイル名（アルバムの場合は複数のファイル名）
・ウォーターマーキング命令・ウォーターマーキング・パラメータ（透かしに含める情報）

【0206】ウォーターマーキング処理808の完了時に、ジョブは、必要な入力が使用可能である場合には前処理および圧縮処理809のキューに入れられ、そうでない場合には、処置／情報待機中製品処理801のキューに入れられる。

【0207】9. 前処理および圧縮処理809前処理および圧縮処理809は、まず必要な前処理を実行し、コンテンツ113を指定された圧縮レベルに符号化する。このキューにジョブを入れると、実際には、複数のキュー項目が作成される。ジョブは、製品の所望の圧縮レベルごとに作成される。符号化処理は、複数のシステム上で並列に実行することができる。このツールは、入力として下記を必要とする。

・ウォーターマーキングされたコンテンツ・ファイル名（コンテンツ113がアルバムの場合は複数のファイル名）
・製品の品質レベル（事前に構成することができる）
・圧縮アルゴリズム（事前に構成することができる）
・製品ジャンル（プリプロセッサが必要とする場合）

【0208】符号化処理の完了時に、ジョブは、ワーク・フロー・ルールによって構成されている場合にはコンテンツ品質管理処理810のキューに入れられる。そうでない場合には、ジョブは、暗号化処理811のキューに入れられる。

【0209】符号化ツールのサード・パーティ・プロバイダが、オーディオなどのコンテンツ113の処理済みの比率を表示する方法または、選択されたコンテンツ113の選択全体の比率としてのコンテンツ113の符号化された量を示す方法を提供しない場合には、図14に、図11のコンテンツ前処理および圧縮ツールのディジタル・コンテンツの符号化率を判定する方法の流れ図1100が示されている。この方法は、所望の符号化アルゴリズムおよびビット率の選択から開始される（ステップ1101）。次に、照会を行って、このアルゴリズムおよび符号化率が、前に計算された率係数を有するかどうかを判定する（ステップ1102）。率係数とは、特定の符号化アルゴリズムおよび特定のビット率に関して圧縮の割合を決定するのに使用される係数である。前に計算された率係数が記憶されていない場合には、コンテンツ113のサンプルを、所定の長さの時間だけ符号化する。好ましい実施形態の所定の時間期間は、2～3秒である。この所定の時間期間の符号化の割合を、新しい率係数R_{NEW}の計算に使用する。時間の長さおよび符号化されたコンテンツ113の量がわかっている場合の新しい率係数R_{NEW}の計算は、R_{NEW}＝（符号化されたディジタル・コンテンツの長さ）／（時間の長さ）である（ステップ1108）。コンテンツ113を符号化し、符号化状況を、前に計算した率係数R_{NEW}を使用して表示する（ステップ1109）。この符号化率係数R_{NEW}を、この符号化アルゴリズムおよび符号化ビット率に関する将来の使用のために記憶する（ステップ1107）。選択されたアルゴリズムが、前に計算された率係数R_{STORED}を有する場合、ステップ1103に進む。コンテンツ113を符号化し、前に計算した率係数R_{STORED}を使用して進捗を表示する（ステップ1104）。その間に、現在の率係数$R_{current}$を、選択されたアルゴリズムおよびビット率について計算する（ステップ1105）。この現在の率係数$R_{current}$を使用して、記憶された率係数を、R_{NEW}＝（R_{STORED}＋$R_{current}$）の平均に更新する（ステップ1106）。率係数の反復更新によって、特定の符号化アルゴリズムおよびビット率の後続の使用のたびに、符号化率の判定をますます正確にすることができる。新しい率R_{NEW}を、将来の使用のために記憶する（ステップ1107）。現在の率係数$R_{current}$が、前に記憶された率係数R_{STORED}の、所与の範囲または閾値による範囲の外にある場合には、R_{STORED}の更新を行わわなくてもよい。

【0210】この場合、符号化状況の表示を提示することができる。符号化状況には、現在の符号化率と共に、符号化率およびコンテンツ113のファイルの全長に基づく進行状況バーとして表示される全コンテンツ113の比率の表示が含まれる。符号化状況には、符号化の残り時間も含めることができる。符号化の残り時間は、計算された符号化率$R_{current}$をコンテンツ113のファイルの全長で割ることによって計算することができる。符号化状況は、別のプログラムに転送することができ、このプログラムが、呼出し元の処理を呼び出すことができる。これは、符号化に対するスーパーバイザ・プログラムまたは符号化に共依存するプログラムを操作し、より効率的な処理のためにバッチ化するのを助けることができる。代替実施形態では、符号化に、ウォーターマーキングのステップを含めることができることを理解されたい。

【0211】10. コンテンツ品質管理処理810コンテンツ品質管理処理810は、機能において監視公開処理806に類似する。これは、誰かがこれまでに実行されたコンテンツ処理の品質を検証できるようにする、任意選択のステップである。これは、ウォーター

マーキング処理808および前処理および圧縮処理809の符号化部分の完了以外の依存性を有しない。コンテンツ品質管理処理810の完了時には、以下のオプションが使用可能である。
・ジョブを解放し、暗号化処理811のキューに入れることができる。
・コメントを付加することができ、1つまたは複数のジョブを、前処理および圧縮処理809のキューにもう一度入れることができる。
【0212】最後のオプションは、曲ファイルの符号化されていないウォーターマーキングされた版が、コンテンツ品質管理処理810の後まで使用可能であることを必要とする。
【0213】11. 暗号化処理811暗号化処理811は、適当なセキュア・ディジタル・コンテンツ電子配布権利管理機能を呼び出して、ウォーターマーキング／符号化された曲ファイルのそれぞれを暗号化する。この処理は、他のすべてのオーディオ処理の完了以外の依存性を有しない。暗号化処理811処理の完了時に、ジョブは、コンテンツSC作成処理812のキューに入れられる。
【0214】12. コンテンツSC作成処理812コンテンツSC作成処理812の処理では、いくつかのメタデータ・ファイルをコンテンツSC630に含めることが必要になる場合がある。コンテンツ113以外のファイルが必要になる場合には、それらのファイルを集め、SCパッカー処理を呼び出して、作成されるコンテンツ113（たとえば曲）の圧縮レベルごとにコンテンツSC630を作成する。コンテンツSC作成処理812の完了時に、曲は、定義済みのワーク・フロー・ルールに基づいて、最終品質保証処理813またはコンテンツ分散処理814のいずれかのキューに入れられる。
【0215】13. 最終品質保証処理813最終品質保証処理813は、関連するメタデータSCおよびコンテンツSC630の間の相互参照検査を可能にして、それらが正しく調和することと、それらに含まれるすべての情報およびコンテンツ113が正しいことを検証する、任意選択のステップである。最終品質保証処理813の完了時に、ジョブは、コンテンツ分散処理814のキューに入れられる。問題が見つかった場合には、ジョブは、ほとんどの場合に、失敗した段階のキューにもう一度入れられなければならない。この段階でのリワークは、はるかにコストがかかる。というのは、製品が、問題の修正に必要な再処理のほかに、再暗号化および再パックを受けなければならないからである。前の保証段階を使用して、コンテンツ113の品質と、情報の正確さおよび完全性を保証することを強く推奨する。
【0216】14. コンテンツ分散処理814コンテンツ分散処理814の処理は、SCを適当なホスティング・サイトに転送する責任を負う。SCの成功裡の転送の後に、ジョブ完了状況がログ記録され、ジョブは、キューから削除される。SCの転送で問題が発生した場合には、定義済みの回数の再試行の後に、ジョブは、遭遇したエラーと共に、失敗したものとしてワーク・フロー・マネージャ・ツール154内でフラグを立てられる。
【0217】15. ワーク・フロー・ルール図11のワーク・フロー・ルールは、次のように3つの主要なシステムで動作する。
A: ワーク・フロー・マネージャ・ツール1541. 新規コンテンツ要求処理8022. 処置／情報待機中製品処理8013. 最終品質保証処理8134. コンテンツ分散処理814B:メタデータ同化および入力ツール1611. 自動メタデータ獲得処理8032. 手動メタデータ入力処理8043. 監視公開処理8064. メタデータSC作成処理807C:コンテンツ処理ツール1551. ウォーターマーキング処理808（著作権データが必要）
2. 前処理および圧縮処理8093. コンテンツ品質管理処理8104. 暗号化処理8115. コンテンツSC作成処理812【0218】ワーク・フローコンテンツ113選択操作員が、新しい製品を入力し、これがA1（新規コンテンツ要求処理802）のキューに入れられた状態で開始される。
A1: コンテンツ113選択操作員が、その製品をワーク・フロー・マネージャ・ツール154に公開する時に、その製品がB1（自動メタデータ獲得処理803）のキューに入れられる。
A2: ステップB1（自動メタデータ獲得処理803）または、ステップB2（手動メタデータ入力処理804）または、ステップB3（監視公開処理806）から来る ステップBefore（メタデータSC作成処理807）への途中 [暗号化鍵が必要]。
ステップBefore（メタデータSC作成処理807）から来る ステップA3（最終品質保証処理813）またはステップA4（コンテンツ分散処理814）のいずれかへの途中 [コンテンツSC630が必要]。
ステップC1（ウォーターマーキング処理808）から来る ステップC2（前処理および圧縮処理809）への途中 [前処理および圧縮処理809用のメタデータが必要]。
ステップC4（暗号化処理811）から来る ステップC5（コンテンツSC作成処理812）への途中 [コンテンツSC630パッキング用のメタデータが必要]。
ステップC5（コンテンツSC作成処理812）から来る ステップA3（最終品質保証処理813）またはステップA4（コンテンツ分散処理814）のいずれかへの途中 [メタデータSC620が必要]。
A3: ステップA3（最終品質保証処理813）の後、キューB2（手動メタデータ入力処理804）または、キューB3（監視公開処理806）または、品質保証操作員の必要に応じたキューに入れる。
A4: ステップA4（コンテンツ分散処理814）の後、この製品についてワーク・フロー・マネージャ・ツール154が終了する。
B1: ステップB1（自動メタデータ獲得処理803）の後、if ステップC1（ウォーターマーキング処理808）に必要なメタデータが存在する then この製品を表す項目をキューC1に置く。（以下の論理も実行する）
if 1－必要なメタデータのどれかが欠けているか、2－手動メタデータ供給者に向けられたコメントがあるのいずれか then この製品をキューB2（手動メタデータ入力処理804）にも置く、else if この製品について監視公開が要求された then 製品をキューB3（監視公開処理806）に置く、else if 製品が、要求された品質レベルのすべてについてコンテンツ処理ツール155からのすべての情報を有する then 製品をキューBefore（メタデータSC作成処理807）に置く、else 暗号化鍵が必要として製品にフラグを立て、製品をキューA2（処置／情報待機中製品処理801）に置く。
B2: ステップB2（手動メタデータ入力処理804）中に、if ステップC1（ウォーターマーキング処理808）が終了しておらず and ステップC1に必要なメタデータが存在する then この製品を表す項目をキューC1に置く。（以下の論理も実行する）
if ステップC2（前処理および圧縮処理809）に必要なメタデータが供給されたばかりである then（以下の論理も実行する）
if メタデータ同化および入力ツール161によって収集することができるメタデータのすべてが存在する thenif この製品について監視公開が要求された then 製品をキューB3（監視公開処理806）に置くelseif コンテンツ処理ツール155のステップC4（暗号化処理811）からのすべての情報が存在する then この製品をキューBefore（メタデータSC作成処理807）に置くelse 暗号化鍵が必要として製品にフラグを立て、この製品をキューA2（処置／情報待機中製品処理801）に置く。
elseif メタデータ提供者が強制監視公開を要求した then この製品をキューB3（監視公開処理806）に置くelse 何もしない（製品をキューB2（手動メタデータ入力処理804）に保持する）。
B3: ステップB3（監視公開処理806）中に、if この操作員が、製品をステップB2（手動メタデータ入力処理804）に送り返す then 製品をキューB2に置く。
else if この操作員が製品を公開する thenif コンテンツ処理ツール155のステップC4（暗号化処理811）からのすべての情報が存在する then この製品をキューBefore（メタデータSC作成処理）に置くelse 暗号化鍵が必要として製品にフラグを立て、この製品をキューA2（処置／情報待機中製品処理801）に置く。
else 製品はキューB3（監視公開処理806）にとどまる。
Before: ステップBefore（メタデータSC作成処理807）の後に、製品にメタデータがパックされたことのフラグを立てるif（製品／品質レベル）タプルのすべてがパックされた thenif コンテンツ・プロバイダ101の構成でSCの品質保証が指定されている then この

製品をキューA3（最終品質保証処理813）に置くelse この製品をキューA4（コンテンツ分散処理814）に置く。
else コンテンツ113SCが必要として製品にフラグを立て、この製品をキューA2（処置／情報待機中製品処理801）に置く。
C1：ステップC1（ウォーターマーキング処理808）の後に、if ステップC2（前処理および圧縮処理809）に必要なメタデータが存在する then（製品／品質レベル）タプルごとに項目を作成し、それらをキューC2に置く、else 前処理／圧縮用のメタデータが必要として製品にフラグを立て、この製品をキューA2（処置／情報待機中製品処理801）に置く。
C2：ステップC2（前処理および圧縮処理809）の後に、if コンテンツ・プロバイダ101の構成でコンテンツ品質管理処理810が指定されている then この（製品／品質レベル）タプルをキューC3（コンテンツ品質管理処理810）に置く、else この（製品／品質レベル）タプルをキューC4（暗号化処理811）に置く。
C3：ステップC3（コンテンツ品質管理処理810）の後に、この（製品／品質レベル）タプルをキューC4（暗号化処理811）に置く。
C4：ステップC4（暗号化処理811）の後に、必要な情報（すなわち、この処理によって生成され、コンテンツ113の暗号化に使用された対称鍵623）をメタデータ同化および入力ツール161に供給する。
if コンテンツSC630に必要なすべてのメタデータが存在するthen この（製品／品質レベル）タプルをキューC5（コンテンツSC作成処理812）に置く、else コンテンツSC630パッキング用のメタデータが必要として製品にフラグを立て、この（製品／品質レベル）タプルをキューA2（処置／情報待機中製品処理801）に置く。
C5：ステップC5（コンテンツSC作成処理812）の後に、この品質レベルのコンテンツ113がパックされたことのフラグを品質レベルに立てるif（製品／品質レベル）タプルのすべてがパックされた thenif 製品にメタデータがパックされたことのフラグが立てられている thenif コンテンツ・プロバイダ101の構成でSCの品質保証が指定されている then この製品をキューA3（最終品質保証処理813）に置くelse この製品をキューA4（コンテンツ分散処理814）に置くelse メタデータSC620が必要として製品にフラグを立て、この製品をキューA2（処置／情報待機中製品処理801）に置く。
else（すべての（製品／品質レベル）タプルがパックされてはいない） 何もしない（別の（製品／品質レベル）タプルが処置のトリガになる）。
【0219】C. メタデータ同化および入力ツールメタデータは、コンテンツ113を記述するデータ、たとえば、音楽では、レコーディングのタイトル、アーティスト、作者／作曲者、プロデューサ、およびレコーディングの長さからなる、以下の説明は、音楽のコンテンツ113に基づくが、当業者は、他のコンテンツ・タイプ、たとえばビデオ、プログラム、マルチメディア、映画、および同等物が、本発明の真の範囲および意味に含まれることを理解されたい。
【0220】このサブシステムは、製品の販売を促進するのを助けるためにコンテンツ・プロバイダ101が電子ディジタル・コンテンツ商店103に供給するデータ（たとえば、音楽の場合、このアーティストによるサンプル・クリップ、このアーティストの経歴、このレコーディングが含まれるアルバムのリスト、このアーティストまたは製品に関連するジャンル）、購入した製品に関してコンテンツ・プロバイダ101がエンドユーザに供給するデータ（たとえば、アーティスト、プロデューサ、アルバム・カバー、トラック長）、およびコンテンツ・プロバイダ101がエンドユーザに提供したい異なる購入オプション（使用条件517）を集める。データは、メタデータSC620にパックされ、電子ディジタル・コンテンツ商店103が入手できるようにされる。これを達成するために、以下のツールを提供する。・自動メタデータ獲得ツール・手動メタデータ入力ツール・使用条件ツール・監視公開ツール【0221】これらのツールを用いると、コンテンツ・プロバイダ101が、ワーク・フロー・マネージャ154に関して上で説明した処理を実施できるようになる。本明細書で説明するツールは、好ましい実施形態ではJavaに基づくツールキットであるが、C／C＋＋、アセンブラおよび同等物などの他のプログラミング言語を使用することができる。
【0222】1. 自動メタデータ獲得ツール自動メタデータ獲得ツールは、上で説明した自動メタデータ獲得処理803を実施する能力をユーザに与える。自動メタデータ獲得ツールは、コンテンツ・プロバイダ101のデータベース160にアクセスし、操作員の支援なしでできる限り大量のデータを取り出すのに使用される。この処理を自動化するための構成方法が使用可能である。コンテンツ・プロバイダ101は、デフォルトのメタデータ・テンプレートを調整して、コンテンツ・プロバイダ101がエンドユーザに供給したいデータのタイプ（たとえば、作曲者、プロデューサ、伴奏者、トラック長）と、コンテンツ・プロバイダ101が電子ディジタル・コンテンツ商店103に供給する販売促進データのタイプ（たとえば、音楽の例では、このアーティストによるサンプル・クリップ、このアーティストの経歴、このレコーディングが含まれるアルバムのリスト、このアーティストに関連するジャンル）を識別することができる。デフォルトのメタデータ・テンプレートには、エンドユーザ装置109が必要とするデータ・フィールド、エンドユーザ装置109に任意選択として供給することができるデータ・フィールド、および、アーティスト、アルバム、またはシングルの販売を促進する、電子ディジタル・コンテンツ商店103を対象とするデータ・フィールドのサンプルの組が含まれる。
【0223】コンテンツ・プロバイダ101のデータベース160からテンプレート・データ・フィールドを抽出するために、自動メタデータ獲得ツールは、データのタイプ（たとえば作曲者、プロデューサ、アーティストの伝記）を、そのデータを見つけることができるデータベース内の位置にマッピングするテーブルを使用する。コンテンツ・プロバイダ101のそれぞれが、彼らの環境のためのマッピング・テーブルを指定するのを助ける。
【0224】自動メタデータ獲得ツールは、コンテンツ・プロバイダ101のメタデータ・テンプレートおよびマッピング・テーブルを使用して、コンテンツ・プロバイダ101のデータベース160から入手できるすべてのデータを獲得する。各製品の状況は、自動メタデータ獲得処理803の結果を用いて更新される。必要なデータが欠けている製品は、手動メタデータ入力処理804のキューに入れられ、そうでない製品は、メタデータSC620にパックするために使用可能になる。
【0225】2. 手動メタデータ入力ツール手動メタデータ入力ツールは、上で説明した手動メタデータ入力処理804を実施する能力をユーザに与える。手動メタデータ入力ツールを用いると、正しく許可された操作員が、欠けているデータを提供することができるようになる。欠けているデータが入手不能であると操作員が判定した場合には、操作員は、製品にコメントを付加し、監視公開を要求することができる。コンテンツ・プロバイダ101は、品質保証のために、製品が監視公開されることを要求することができる。必要なデータのすべてが存在するようになった後、監視公開が要求されなかった場合に、製品は、メタデータSC620へのパックのために使用可能になる。
【0226】3. 使用条件ツール使用条件ツールは、上で説明した使用条件処理805を実施する能力をユーザに与える。電子配布を使用する、販売またはレンタル（制限付き使用）に関するコンテンツ113の提供の処理には、一連のビジネス決定が含まれる。コンテンツ・プロバイダ101は、どの圧縮レベルでコンテンツ113を使用可能にするかを決定する。その後、コンテンツ113の圧縮され符号化された版のそれぞれについて、1つまたは複数の使用条件が指定される。使用条件のそれぞれでは、コンテンツ113の使用に関する、エンドユーザの権利とエンドユーザに対する制限が定義される。
【0227】コンテンツ処理ツール155の一部として、1組の使用条件（エンドユーザの権利および制限）が、製品に付加される。
【0228】使用条件では、以下が定義される。
1. この使用条件が適用される、コンテンツ113の圧縮符号化された版。
2. この使用条件に含まれるユーザのタイプ（たとえば、会社、個人消費者）
3. この使用条件で、コンテンツ113の購入またはレンタルが許可されるかどうか。
レンタル・トランザクションの場合：・レンタルの期間を制限するのに使用される測定単位（たとえば、日数、再生回数）。
・その後にコンテンツ113が再生されれなくなる上の単位の数。
購入トランザクションの場合：・エンドユーザが作成を許可される再生可能なコピーの数。

・エンドユーザがそれらのコピーを作成できる媒体の種類（たとえば、CD－R（CD－Recordable）、ミニディスク、パーソナル・コンピュータ）。
4. 購入／レンタル・トランザクションの発生が許可される時間期間（すなわち、エンドユーザは、最初の使用可能性日付の後、使用可能性の最後の日付の前に限って、この使用条件の条件の下で購入／レンタルを行うことができる）。
5. そこからエンドユーザがこの購入（またはレンタル）の取引を行うことができる国。
6. この使用条件の下での購入／レンタル・トランザクションの価格7. ウォーターマーキング・パラメータ。
8. クリアリングハウス105の通知を必要とするイベントのタイプ。
【0229】使用条件の組の例コンテンツ・プロバイダ101は、1997年第4四半期中に有名な子供の歌手による子供の曲の再リリースに対する北米市場の受入をテストすると決定することができる。このテストでは、その曲を、2つの異なる圧縮符号化版すなわち、384Kbpsおよび56kbpsで入手可能にする。384Kbps版は、購入（およびミニディスクへの1回のコピー）またはレンタル（2週間）が可能であり、56Kbps版は、購入のみが可能（コピー作成は不可）である。ウォーターマーキング命令は、どの購入／レンタルについても同一であり、コンテンツ・プロバイダ101は、クリアリングハウス105が、作成されるすべてのコピーをカウントすることを望んでいる。これによって、次のような使用条件が作成されるはずである。
【0230】
【表10】

	使用条件1	使用条件2	使用条件3
圧縮され符号化された版	384Kbps	384Kbs	56Kbps
ユーザのタイプ	個人消費者	個人消費者	個人消費者
トランザクションのタイプ	購入	レンタル	購入
使用可能性日付	1997年10月1日～1997年12月31日	1997年10月1日～1997年12月31日	1997年10月1日～1997年12月31日
国	アメリカおよびカナダ	アメリカおよびカナダ	アメリカおよびカナダ
ウォーターマーキング	標準	標準	標準
通知イベント	コピー処理	なし	なし
コピーの数	1	0	0
コピー先媒体	ミニディスク	適用不能	適用不能
レンタルの期間	適用不能	１４日間	適用不能
価格	価格1	価格2	価格3

【0231】4. メタデータSC620の諸部分下記は、メタデータ同化および入力ツール161がメタデータSC620に含めるために収集するデータの種類の一部である。機能および宛先によって、データをSC部分にグループ化する試みが行われている。
【0232】
【表11】
製品ＩＤ [src: コンテンツ・プロバイダ;]
[dest: すべて;]
ライセンス交付先レーベル会社 [dest: EMS; エンドユーザ;]
ライセンス所有レーベル会社 [dest: EMS; エンドユーザ;]
このオブジェクトのソース（発行者）（サブライセンス所有レーベル会社）
[dest: すべて;]
オブジェクトのタイプ（すなわち、単一オブジェクトまたはオブジェクトの配列）
オブジェクトＩＤ [dest: すべて;]
ＩＳＲＣ（International Standard Recording Code）
ＩＳＭＮ（International Standard Music Number）

使用条件 (src: コンテンツ・プロバイダ; dest: EMS, エンドユーザ, クリアリングハウス１０５)
購入された使用条件 (src: EMS; dest: エンドユーザ, クリアリングハウス１０５)
オブジェクトの使用に関する使用条件（消費者の制限および権利）の組
（サウンド・レコーディング）
使用条件の配列内の個々の項目
この使用条件が適用されるコンテンツ１１３の圧縮符号化された版
この使用条件でコンテンツ１１３の購入またはレンタルが許可されるかどうか
レンタル・トランザクションの場合:
レンタルの期間を制限するのに使用される測定単位（たとえば日数、再生回数）
その後にコンテンツ１１３が再生されなくなる上の単位の数
購入トランザクションの場合:
エンドユーザが作成を許可される再生可能なコピーの数
エンドユーザがそれらのコピーを作成できる媒体の種類（たとえば、ＣＤ－Ｒ（CD-Recordable）、ミニディスク、パーソナル・コンピュータ）。
購入／レンタル・トランザクションの発生が許可される時間期間
（すなわち、エンドユーザは、最初の使用可能性日付の後、使用可能性の最後の日付の前に限って、この使用条件の条件の下で購入／レンタルを行うことができる）

【表12】

エンドユーザがこの購入（またはレンタル）の取引を行うことができる国へのポインタ
この使用条件の下での購入／レンタル・トランザクションの価格
暗号化されたウォーターマーキング命令およびウォーターマーキング・パラメータへのポインタ
クリアリングハウス１０５の通知を必要とするイベントのタイプへのポインタ

購入データ（暗号化；オプション情報；src: EMS; dest: エンドユーザ，クリアリングハウス１０５）
購入日付
購入価格
請求先の名前および住所
消費者の名前および住所
消費者の国（最適推測）

メタデータ１（src: コンテンツ・プロバイダ; dest: EMS, エンドユーザ）
an array of {
著作権情報
作曲に関する
サウンド・レコーディングに関する
曲名
主要なアーティスト
}
a pointer to {
アートワーク（たとえばアルバム・カバー）；
アートワークのフォーマット（たとえばＧＩＦ、ＪＰＥＧ）；
}

オプション情報:

【表13】
an array of 追加情報 {
作曲者
発行者
プロデューサ
伴奏者
レコーディングの日付
公開の日付
歌詞
トラック名（説明）／トラック長
このレコーディングが含まれるアルバムのリスト
ジャンル
}

メタデータ２（src: コンテンツ・プロバイダ; dest: EMS）
an array of それぞれが同一のサウンド・レコーディングの異なる品質レベルを表す構造体 {
サウンド・レコーディング;
サウンド・レコーディングの品質レベル;
（おそらく圧縮された）サウンド・レコーディングのサイズ（バイト単位）；
}

メタデータ３（src: コンテンツ・プロバイダ; dest: EMS, エンドユーザ）
オプション情報:

販売促進材料:
a pointer to アーティスト販売促進材料 {
アーティストのウェブ・サイトへのＵＲＬ;
アーティストのバックグラウンドの説明;
アーティスト関連のインタビュー（インタビューのフォーマット（たとえばテキスト、オーディオ、ビデオ）と共に）；
レビュー（レビューのフォーマット（たとえばテキスト、オーディオ、ビデオ）と共に）；
サンプル・クリップ（およびそのフォーマットおよび圧縮レベル）；
最近および今後のコンサート／出演／イベント　その日付および場所;
}

【表14】
a pointer to アルバム販売促進材料 {
サンプル・クリップ（およびそのフォーマットおよび圧縮レベル）;
プロデューサ、作曲家、映画／演奏／出演、アルバムのメイキングなどの背景説明;
非アーティスト関連のインタビュー（インタビューのフォーマット（たとえばテキスト、オーディオ、ビデオ）と共に）;
レビュー（レビューのフォーマット（たとえばテキスト、オーディオ、ビデオ）と共に）;
ジャンル;
}
シングル販売促進:
サンプル・クリップ（およびそのフォーマットおよび圧縮レベル）
プロデューサ、作曲家、映画／演奏／出演、シングルのメイキングなどの背景説明
レビュー（レビューのフォーマット（たとえばテキスト、オーディオ、ビデオ）と共に）

【0233】5. 監視公開ツール監視公開ツールは、上で説明した監視公開処理806を実施する能力をユーザに与える。監視公開の権限を有するものとしてコンテンツ・プロバイダ101によって指定された個人は、監視公開を待っている製品（すなわち、監視公開処理806のキューにある製品）を呼び出し、そのコンテンツ113およびそれに付随するコメントを検査することができ、下記のいずれかを行うことができる。コンテンツ113を承認し、メタデータSC620へのパックのために製品を公開するか、必要な訂正を行い、メタデータSC620へのパックのために製品を公開するか、行うべき訂正処置を指定するコメントを追加し、製品を手動メタデータ入力処理804に再サブミットする。
【0234】もう1つの実施形態では、SCの作成の後に、SCのコンテンツ113をオープンでき、完全性および正確度について検査でき、その時点で、小売りチャネルへの製品の公開に関する最終承認を与えるか拒否することができる、もう1つの任意選択の品質保証ステップがある。
【0235】D. コンテンツ処理ツールコンテンツ処理ツール155は、実際には、ディジタル・コンテンツ・ファイルを処理してウォーターマーキングされ符号化され暗号化されたコンテンツのコピーを作成するのに使用されるソフトウェア・ツールの集合である。これらのツールは、業界標準のディジタル・コンテンツ処理ツールを利用して、ウォーターマーキング技術、符号化技術、および暗号化技術が進歩した時にそれらのプラグ可能な交換を可能にする。選択された業界ツールを、コマンド・ライン・システム呼出しインターフェースを介してロードでき、パラメータを渡すことができるか、DLLインターフェースを介して機能を呼び出すことができるツールキットを提供できる場合には、コンテンツ処理を、ある程度まで自動化することができる。各ツールに対するフロント・エンド・アプリケーションが、次に使用可能なジョブについてコンテンツ処理ツール155内の適当なキューを照会し、必要なファイルおよびパラメータを取り出し、業界標準のコンテンツ処理ツールをロードして、必要な機能を実行する。タスクの完了時に、ツールが終了状況を報告しない場合には、キューに対する手動の更新が必要になる可能性がある。
【0236】コンテンツ処理ツール155の一般的な版を説明するが、カスタマイズが可能である。コンテンツ処理ツール155は、Java、C／C＋＋、または同等のソフトウェアで記述することができる。コンテンツ処理ツール155は、ディスケット、CDを含むすべてコンピュータ可読手段によるかウェブ・サイトを介して配布することができる。
【0237】1. ウォーターマーキング・ツールウォーターマーキング・ツールは、上で説明したウォーターマーキング処理808を実施する能力をユーザに与える。このツールは、オーディオ・ウォーターマーキング技術を使用して、コンテンツ113所有者の著作権情報を曲ファイルに加える。実際に書き込まれる情報は、コンテンツ・プロバイダ101と、選択された特定のウォーターマーキング技術によって決定される。この情報は、フロント・エンド・ウォーターマーキング・ツールから使用可能であり、その結果、そのツールは、この情報をウォーターマーキング機能に正しく渡すことができる。これは、たとえば曲のオーディオ・ファイルを処理できるようにする前に、メタデータ同化および入力ツール161が確実にこの情報を獲得するようにするために、メタデータ同化および入力ツール161に対する同期化要件を課す。この曲は、ウォーターマーキング情報が得られるまでは、オーディオ処理のために使用可能にはならない。
【0238】透かしは、作成される曲の符号化のすべてに共通なので、オーディオ処理の第1ステップで適用される。透かしが符号化技術に耐える限り、ウォーターマーキング処理は、曲ごとに1回だけ行えば十分である。
【0239】さまざまなウォーターマーキング技術が、既知であり、市販されている。しかし、フロント・エンド・ウォーターマーキング・ツールは、さまざまな業界ウォーターマーキング・ツールをサポートする能力を有する。
【0240】2. 前処理および圧縮ツール前処理および圧縮ツールは、上で説明した前処理および圧縮処理809を実施する能力をユーザに与える。オーディオ符号化には、2つの処理が含まれる。符号化は、基本的に、音楽コンテンツの例ではPCMオーディオ・ストリームに対する、ロッシイ圧縮アルゴリズムの適用である。エンコーダは、通常は、要求されるオーディオ品質のレベルに基づいて、さまざまな再生ビット・ストリーム速度を生成するように調整することができる。高品質は、大きいファイル・サイズをもたらし、ファイル・サイズは、高品質のコンテンツ113では非常に大きくなる可能性があるので、高品質のコンテンツ113のダウンロード時間は、非常に長くなり、時には標準的な28800bpsモデムでは事実上使用不能になる可能性がある。
【0241】したがって、コンテンツ・プロバイダ101は、ダウンロードのために何時間も待ちたくない気短または低帯域幅の顧客と、高品質のコンテンツ113だけを購入するか高速接続を有するかのいずれかであるハイファイ愛好家または高帯域幅の顧客の両方の歓心を買うために、ダウンロード用にさまざまなディジタル・コンテンツ品質を提供することができる。
【0242】圧縮アルゴリズムは、コンテンツ113の低ビット・レート再生を生成するための技術において変化がある。技術は、アルゴリズム（すなわち、MPEG、AC3、ATRAC（登録商標））と圧縮レベルの両方によって変化する。より高いレベルの圧縮を達成するためには、通常は、圧縮アルゴリズムに渡す前に、データを、低いサンプリング・レートで再サンプリングする。忠実性の消失が少ないより効率的な圧縮を可能にするため、または、一部の周波数範囲の劇的なドロップアウトを防ぐために、ディジタル・コンテンツが、時々、一部の周波数の等化レベルに対する調整またはレコーディングの動特性に対する調整を必要とする場合がある。コンテンツ前処理要件は、圧縮アルゴリズムと必要な圧縮のレベルに直接に関係する。場合によっては、コンテンツ113のスタイル（たとえば音楽ジャンル）を、前処理要件を決定するための基礎として成功裡に使用することができる。というのは、同一のジャンルからの曲が、通常は類似した動特性を有するからである。一部の圧縮ツールでは、これらの前処理機能が、符号化処理の一部になっている。それ以外の圧縮ツールでは、所望の前処理が、圧縮の前に実行される。
【0243】販売用のダウンロード可能なオーディオ・ファイルのほかに、各曲は、低ビット・レート（LBR）ストリーミング・プロトコルを介して曲をサンプリングできるようにするためにLBR符号化されたクリップも有する。このLBR符号化も、コンテンツ処理ツール15

5の責任である。このクリップは、コンテンツ・プロバイダ101によって別のPCMファイルとして、またはオフセットおよび長さのパラメータとしてのいずれかで供給される。
【0244】ウォーターマーキングと同様に、符号化ツールは、DLLまたはコマンド・ライン・システム呼出しインターフェースを介してロードでき、前処理および圧縮に必要なすべてのパラメータを渡せることが望まれる。フロント・エンド符号化ツールは、たとえばコンテンツが音楽の場合で、曲のジャンルがコンテンツ・プロバイダのデータベース160から獲得されると判定された場合に、オーディオ前処理を実行する前に、メタデータ同化および入力ツール161との同期化要件を有する場合がある。これは、選択された符号化ツールと、曲のジャンルがどれほど不確定であるかに依存する。コンテンツ・プロバイダ101が、曲ごとに符号化された品質レベルの選択を変更する場合には、この情報も、符号化ステップの前に供給され、メタデータ同化および入力ツール161によって生成されるメタデータと一致する。
【0245】さまざまな高品質符号化アルゴリズムおよびツールが、現在既知である。しかし、フロント・エンド符号化ツールは、さまざまな業界符号化ツールをサポートする能力を有する。
【0246】ここで図15に移ると、本発明による、図11の自動メタデータ獲得ツールの一実施形態の流れ図が示されている。この処理は、コンテンツ・プロバイダ101が検査中の媒体から識別子を読み取ることから開始される。コンテンツの一例が、オーディオCD実施形態である。オーディオCD実施形態では、UPC(統一商品コード)、ISRC(International Standard Recording Code)、ISMN(International Standard Music Number)が使用可能である可能性がある。この識別子は、たとえばオーディオCDの場合はオーディオCDプレイヤ、DVDムービーの場合はDVDプレイヤ、DATレコーディングおよび同等物の場合はDATレコーダなど、コンテンツに適したプレイヤで読み取られる(ステップ1201)。次に、この識別子を使用して、コンテンツ・プロバイダ101のデータベース160をインデクシングする(ステップ1202)。図11で説明したワーク・フロー・マネージャ処理が必要とする情報の一部またはすべてが、データベース160および他の関連ソース内で検索される(ステップ1203)。この情報には、コンテンツ113とそれに関連するメタデータを含めることができる。ステップ1204で、検索された追加情報を使用して、電子的なコンテンツ113を作成するためにワーク・フロー・マネージャ154を始動する。複数のオーディオCDなどの複数の媒体の選択をキューに入れ、自動メタデータ獲得ツールが電子配布用の一連のコンテンツ113を作成できるようにすることが可能であることを理解されたい。たとえば、すべてのコンテンツ113を、一連のCDから作成するか、コンテンツ・プロバイダ101によって検査される1つまたは複数のCDの選択されたトラックから作成することができる。
【0247】代替実施形態では、前処理パラメータを、コンテンツ・プロバイダのデータベース160から自動的に検索することができる。ここで図16を参照すると、本発明による、図11の前処理および圧縮ツールの、前処理パラメータおよび圧縮パラメータを自動的に設定する方法の流れ図が示されている。この実施形態では、コンテンツ113は音楽である。ステップ1301で、コンテンツ処理ツール155で符号化される音楽(コンテンツ113)を選択する。選択された音楽のジャンルを判定する(ステップ1302)。これは、手動で入力するか、図15で説明した処理から検索される追加データなど、他の使用可能なメタデータを使用することによって入力することができる。選択されたオーディオ圧縮レベルおよびオーディオ圧縮アルゴリズムを検査する(ステップ1303)。次に、ジャンル、圧縮設定、および圧縮アルゴリズムによって、どの圧縮パラメータを前処理および圧縮処理809で使用しなければならないかに関するテーブル索引を行う(ステップ1304)。
【0248】3. コンテンツ品質管理ツールコンテンツ品質管理ツールは、上で説明したコンテンツ品質管理処理810を実施する能力をユーザに与える。これは、任意選択のコンテンツ処理ツールであり、品質管理技術者が、符号化されウォーターマーキングされたコンテンツ・ファイルを再検討し、品質判断に基づいてコンテンツ・ファイルを承認または拒絶する機会を提供する。品質管理技術者は、品質が適当になるまで手動前処理調整を行ってコンテンツを再符号化することができ、また、曲に再処理のフラグを立て、問題を記述したメモを付加することができる。
【0249】この処理ステップは、コンテンツ処理ワーク・フローの任意選択ステップまたは必要なステップとして、コンテンツ・プロバイダ101が構成することができる。追加の任意選択の最終品質保証処理813ステップが、このコンテンツのすべてのSC(たとえば、CD上の曲の各SC)のパッケージ化の後に設けられ、この時点で、コンテンツ符号化の品質をテストすることができるが、暗号化およびパッケージ化の前に早期に問題を捕まえることによって、より効率的なコンテンツ処理が可能になる。したがって、コンテンツ品質は、すべての処理の最終的な完了を待つのではなく、このステップで保証されることが非常に望ましい。
【0250】4. 暗号化ツール暗号化ツールは、上で説明した暗号化処理811を実施する能力をユーザに与える。コンテンツ暗号化は、コンテンツ処理ツール155の最終ステップである。符号化ツールによって作成されたコンテンツの版のそれぞれが、ここで暗号化される。暗号化ツールは、SCパッカーの1機能である。SCパッカーは、曲を暗号化するために呼び出され、使用された生成された暗号化鍵を返す。この鍵は、後に、メタデータSC620の作成に使用するためにSCパッカーに渡される。
【0251】E. コンテンツSC作成ツールすべてのメタデータが収集された後に、コンテンツSC作成ツールは、メタデータをその所期の目的に基づくカテゴリにグループ化する。これらのメタデータのグループは、メタデータSC620のメタデータ部分としてSCパッカー・ツールに渡されるファイルに書き込まれる。各部分(ファイル)は、独自の処理要件を有する。関連する曲が処理され、暗号化され、目標宛先(コンテンツ・ホスティング・サイト111のURL)が決定された後に、コンテンツ113のコンテンツSC630を作成する準備が調う。処理が完了し、上で説明したすべての要件を満たすコンテンツ113は、ワーク・フロー・マネージャ154のパッカー・キューにパックのために入れられる。
【0252】コンテンツSC作成ツールは、ここで、メタデータ同化および入力ツール161の前のステップによって作成された必要なファイルのすべてを取り出し、SCパッカー機能を呼び出して、メタデータSC620およびコンテンツSC630を作成する。この処理では、曲ごとに1つのメタデータSC620と複数のコンテンツSC630が作成される。たとえば、コンテンツが音楽の場合に、完全な曲のさまざまな品質レベルに関するオーディオ処理中に作成されたオーディオ・ファイルのそれぞれが、別々のコンテンツSC630にパックされる。サンプル・クリップ用に作成されたオーディオ・ファイルは、メタデータ・ファイルとして渡されて、メタデータSC620に含まれる。
【0253】F. 最終品質保証ツール最終品質保証ツールは、上で説明した最終品質保証処理813を実施する能力をユーザに与える。すべてのSCがコンテンツ・ファイルに関して作成された後に、コンテンツは、最終品質保証検査のために使用可能になる。品質保証は、コンテンツ113準備処理のさまざまな段階で実行することができる。コンテンツ・プロバイダ101は、後の過剰なリワークを避けるために主要なステップのそれぞれが完了した時に品質保証を実行することを選択でき、また、すべてのオーディオ準備処理が完了するまで待ってからすべての品質保証を一度に行うことを選択することができる。後者が選択された場合、品質保証は、この位置で、SCの作成の完了時に実行される。このツールでは、曲の各SCをオープンし、検査し、オーディオを再生することができる。
【0254】発見された問題は、些細なテキスト変更であっても、SCの内部セキュリティ機能に起因して、SCの再作成を必要とする。無用な再処理時間を避けるために、中間の品質保証ステップを使用して、メタデータの精度を保証することと、この特定の品質保証ステップを、この曲に関連するSCの間の適当な相互参照の検証のために予約することを強く推奨する。問題が見つかった場合には、保証者は、曲に付加される問題記述を入力することができ、その曲を、再処理のために適当な処理キューにもう一度入れることができる。状況は、曲のすべての関連するコンポーネントの状況を示すためにワーク・フロー・マネージャ154内で適当に更新される。問題が発見されない場合には、コンテンツ113に、公開の準備ができているものとしてマークをつけるかフラグを立てる。
【0255】G. コンテンツ分散ツールコンテンツ分散ツールは、上で説明したコンテンツ分散処理814を実施する能力をユーザに与

える。コンテンツ113が、公開について承認された後に、コンテンツ113のSCが、コンテンツ分散処理のキューに置かれる。コンテンツ分散ツールは、このキューを監視し、コンテンツ・プロバイダ101によって供給される構成設定に基づいて、SCファイルの即時転送またはSCファイルのグループのバッチ転送を実行する。コンテンツ・プロバイダ101は、任意選択として、手動で解放についてフラグを立てられるまですべてのSCをこのキューに自動的に保持するようにコンテンツ分散ツールを構成することもできる。これによって、コンテンツ・プロバイダ101は、スケジューリングされた公開日の前にコンテンツを準備し、たとえば新曲、映画、またはゲームを公開したくなるまで保持することができるようになる。SCは、定義済みの公開日付に基づいてコンテンツ113へのアクセスを制御することもでき、したがって、コンテンツ・プロバイダ101が、実際にSCの配布を遅らせる必要はないが、この手動公開オプションは、この目的に使用することも、これらの大きいファイルを転送するのに必要なネットワーク帯域幅を制御するのに使用することもできる。

【0256】公開のフラグを立てられた時に、コンテンツ113のコンテンツSC630は、指定されたコンテンツ・ホスティング・サイト111にFTPを介して転送される。メタデータSC620は、FTPを介して、コンテンツ販売促進ウェブ・サイト156に転送される。ここで、SCは、処理とコンテンツ販売促進ウェブ・サイト156への統合が可能になるまで、新しいコンテンツ113のための新規コンテンツ・ディレクトリにステージングされる。

【0257】図21は、本発明による、図11の自動メタデータ獲得ツールの、追加情報を自動的に取り出すための代替実施形態の流れ図である。この処理は、上で図11で説明したものに類似する。しかし、監視公開処理806およびコンテンツ品質管理処理810の品質検査が、品質管理1704と称する1つの品質検査に組み合わされている。品質検査は、メタデータSC作成処理807およびコンテンツSC作成処理812の前に実行される。SC作成の前に品質検査を実行することによって、コンテンツ113および関連するメタデータSC620をアンパックするステップが除去される。さらに、この実施形態では、処置／情報待機中製品処理801のキューが除去されている。ジョブは、要求されている処置に応じて、特定の処理キューに置かれる。たとえば、ジョブが手動メタデータすなわち追加メタデータの入力を必要とする場合には、ジョブは、手動メタデータ入力キューに置かれる。また、自動メタデータ獲得処理803は、新規コンテンツ要求と合併されて、メタデータ同化および入力ツール161およびコンテンツ処理ツール155の前に行われる。最後に、使用条件処理805が、自動メタデータ獲得処理803および手動メタデータ入力処理804の両方で入力されることを指摘することが重要である。これは、使用条件の多くを、自動メタデータ獲得処理803ステップの間に自動的に書き込むことができるからである。

【0258】H. コンテンツ販売促進ウェブ・サイトコンテンツ・プロバイダ101がディジタル・ダウンロードを介する販売のために入手可能にしているものに関する情報を最も効率的に分散し、電子ディジタル・コンテンツ商店103に必要なファイルを得てこのコンテンツ113をその顧客へのダウンロードに使用可能にするために、各コンテンツ・プロバイダ101は、この情報を収納するセキュア・ウェブ・サイトを有する必要がある。これは、販売促進コンテンツを小売業者およびこの情報を必要とする他者に入手可能にするために一部のコンテンツ・プロバイダ101が現在使用している方法に類似する。この種のサービスがすでに存在する場合には、電子ディジタル・コンテンツ商店103がダウンロードを介する販売のために使用可能なコンテンツのリストを見るために行くことができる追加セクションをウェブ・サイトに追加することができる。

【0259】コンテンツ・プロバイダ101は、このサイトの設計およびレイアウトに対する完全な制御を有し、また、セキュア・ディジタル・コンテンツ電子配布システム100用のツールキットの一部として提供されるターンキー・ウェブ・サーバ・ソリューションの使用を選択することができる。このサービス用のそれ自体の設計を実施するために、コンテンツ・プロバイダ101は、そのサイトにアクセスする電子ディジタル・コンテンツ商店103用のメタデータSC620へのリンクを提供するだけでよい。これは、セキュア・ディジタル・コンテンツ電子配布システム100用のツールキットを使用して達成される。選択処理およびどの情報を示すかは、コンテンツ・プロバイダ101の自由裁量である。

【0260】コンテンツ分散ツールからFTPを介して新規コンテンツ・ディレクトリに受信されたメタデータSC620は、コンテンツ販売促進ウェブ・サイト156によって処理される。これらのコンテナは、SCプレビュー・ツールを用いてオープンして、コンテナから情報を表示または抽出することができる。この情報は、HTMLウェブ・ページの更新またはこのサービスによって維持される検索可能データベースへの情報追加に使用することができる。SCプレビュー・ツールは、実際には、電子ディジタル・コンテンツ商店103がメタデータSC620のオープンおよび処理に使用するコンテンツ獲得ツールのサブセットである。詳細については、コンテンツ獲得ツールの節を参照されたい。その後、メタデータSC620ファイルは、コンテンツ販売促進ウェブ・サイト156によって維持される永続ディレクトリに移動されなければならない。

【0261】メタデータSC620がコンテンツ販売促進ウェブ・サイト156に統合された後に、その使用可能性を公表する。コンテンツ・プロバイダ101は、新しいメタデータSC620のそれぞれがサイトに追加されるたびに契約している電子ディジタル・コンテンツ商店103のすべてに通知を送信することができ、また、毎日（または定義された期間ごと）、その日（または期間）に追加されたすべてのメタデータSC620の単一の通知を実行することができる。この通知は、追加されたメタデータSC620を参照するパラメータを含む定義済みのCGI文字列を送信することによって、電子ディジタル・コンテンツ商店103のウェブ・サーバとの標準HTTP交換を介して実行される。このメッセージは、後で説明する電子ディジタル・コンテンツ商店103の通知インターフェース・モジュールによって処理される。

【0262】I. コンテンツ・ホスティングエンターテイメント産業は、CD、映画、およびゲームなどのコンテンツ・タイトルを毎年数千本製作し、現在使用可能な数万本のコンテンツ・タイトルに追加している。セキュア・ディジタル・コンテンツ電子配布システム100は、現在の商店で入手可能なコンテンツ・タイトルのすべてをサポートするように設計されている。

【0263】セキュア・ディジタル・コンテンツ電子配布システム100が日次単位で最終的に顧客にダウンロードすることができるコンテンツ・タイトルの数は、数千または数万になる。大量のタイトルの場合、これは大量の帯域幅を必要とする。コンピュータのディスク空間および帯域幅の必要は、複数のコンテンツ・ホスティング・サイト111を有するスケーラブルな分散実施形態を必要とする。このシステムは、全世界の顧客もサポートする。これは、全世界の顧客への配布を高速化するための海外サイトを必要とする。

【0264】セキュア・ディジタル・コンテンツ電子配布システム100でのコンテンツ・ホスティングは、コンテンツ・プロバイダ101が、それ自体のコンテンツ113をホストするか、共通の施設または施設の組を共用するかのいずれかを可能にするように設計されている。

【0265】セキュア・ディジタル・コンテンツ電子配布システム100でのコンテンツ・ホスティングは、セキュア・ディジタル・コンテンツ電子配布システム100によって提供されるコンテンツ113のすべてを集合的に含む複数のコンテンツ・ホスティング・サイト111と、コンテンツ・プロバイダ101によって提供される現在のヒット作を含む複数の2次コンテンツ・サイト（図示せず）からなる。コンテンツ・ホスティング・サイト111の数は、そのシステムを使用するエンドユーザの数に応じて変化する。2次コンテンツ・サイトは、限られた数の曲をホストするが、システムで使用される帯域幅の大きな比率を表す。2次サイトは、1次サイトのボリュームが最大容量の点まで増えた時にオン・ラインにされる。2次サイトは、ネットワーク・アクセス・ポイント（NAP）の近くに配置することができ、これがダウンロード時間の高速化を助ける。2次サイトは、ダウンロード時間を高速化するために世界中の異なる地理的区域に配置することもできる。

【0266】コンテンツ・プロバイダ101は、それ自体のシステムでコンテンツ113のすべてをホストすることを選択した場合に、追加の2次コンテンツ・サイトの有無を問わず、単一のコンテンツ・ホスティング・サイト111として働くことができる。これによって、コンテンツ・プロバイダ101が、それ自体のスケーラブルな分散システムを構築できるようになる。もう1つの実施形態では、電子ディジタ

ル・コンテンツ商店103も、一部のコンテンツ113についてコンテンツ・ホスティング・サイト111として働くことができる。この実施形態では、電子ディジタル・コンテンツ商店103とコンテンツ・プロバイダ101の間での特殊な金銭上の協定が必要になる。
【0267】1. コンテンツ・ホスティング・サイトコンテンツ113は、本明細書のコンテンツ・プロバイダの節で説明したコンテンツ分配ツールによって、FTPまたはHTTPを介して、または、テープ、CD－ROM、フラッシュ、または他のコンピュータ可読媒体でのコンテンツ配布などのオフライン手段を介して、コンテンツ・ホスティング・サイト111に追加される。コンテンツ・プロバイダ101によって作成されるメタデータSC620に、このコンテンツ113のコンテンツSC630を突きとめるURLを示すフィールドが含まれる。このURLは、コンテンツ・ホスティング・サイト111に対応する。電子ディジタル・コンテンツ商店103は、コンテンツ・プロバイダ101によって許可される場合にオファーSC641でこのURLを変更することができる。エンドユーザ装置109は、コンテンツSC630をダウンロードしたい時に、このコンテンツ・ホスティング・サイト111と通信する。
【0268】エンドユーザ装置109は、ライセンスSC660をコンテンツ・ホスティング・サイト111に送信することによって、コンテンツSC630の要求を開始する。これは、クリアリングハウス105によって返されるライセンスSC660と同一である。ライセンスSC660のディジタル署名を検証して、それが有効なライセンスSC660であるかどうかを判定することができる。それが有効なライセンスSC660である場合には、ダウンロードを開始するか、ダウンロード要求を別のコンテンツ・ホスティング・サイト111にリダイレクトすることができる。
【0269】2. セキュア・ディジタル・コンテンツ電子配布システム100によって提供されるコンテンツ・ホスティング・サイト111セキュア・ディジタル・コンテンツ電子配布システム100の場合、コンテンツ113のダウンロードにどのサイトを使用するかの決定は、コンテンツSC630の最初の要求を受信した1次コンテンツ・サイトによって行われる。このサイトは、以下の情報を使用してこの決定を行う。
・要求されたコンテンツ113をホストする2次コンテンツ・サイトがあるか（セキュア・ディジタル・コンテンツ電子配布システム100が提供するコンテンツ113の大多数は、1次サイトだけに配置される）
・エンドユーザ装置109は、地理的にはどこに配置されているか（この情報は、要求がエンドユーザ装置109で開始された時にエンドユーザ装置109から取得でき、これが、注文SC650内でクリアリングハウス105に渡される）
・適当な2次サイトが動作しているか（2次サイトがオフラインになっている場合がある）
・2次サイトの負荷はどれほどか（2次サイトが活動で手一杯の場合には、より負荷の低い別のサイトを選択することができる）
【0270】コンテンツSC630をエンドユーザ装置109に送信する前に、エンドユーザの要求に対する分析および検証を実行する。コンテンツ113のダウンロードに使用されたすべてのライセンスSCのIDのデータベースを保持する。このデータベースを検査して、エンドユーザ装置109が、購入したコンテンツ113の各部分の要求だけを行うようにすることができる。これによって、悪意を持ったユーザがコンテンツ・ホスティング・サイト111の速度低下をもくろんでコンテンツ・ホスティング・サイト111に繰り返しアクセスすることができなくなり、コンテンツSC630の許可されないダウンロードができなくなる。
【0271】2次コンテンツ・サイトへのコンテンツ113の昇格および降格は、コンテンツ113の個々の部分に対する顧客需要に基づいて定期的に行われる。
【0272】コンテンツ・ホスティング・ルータコンテンツ・ホスティング・ルータ（図示せず）は、コンテンツ・ホスティング・サイト111に存在し、コンテンツ113のダウンロードを待っているエンドユーザからのすべての要求を受信する。コンテンツ・ホスティング・ルータは、エンドユーザの要求に対する検証検査を実行して、エンドユーザが実際にコンテンツ113を購入したことを保証する。2次コンテンツ・サイトの状況に関する、そこにあるコンテンツ113とその現在の状況とを含むデータベースが維持される。この現在の状況には、そのサイトでの活動の量と、サイトが保守のためにダウンしているかどうかが含まれる。
【0273】コンテンツ・ホスティング・ルータへの唯一のインターフェースは、コンテンツ113のダウンロードが要求される時にエンドユーザ装置109によって送信されるライセンスSC660である。ライセンスSC660には、ユーザがコンテンツ113のダウンロードを許可されることを示す情報が含まれる。
【0274】2次コンテンツ・サイト2次コンテンツ・サイト（図示せず）は、セキュア・ディジタル・コンテンツ電子配布システム100の人気のあるコンテンツ113をホストする。これらのサイトは、地理的に全世界に分散し、ダウンロード時間を改善するためにネットワーク・アクセス・ポイント（NAP）の近くに配置される。これらのサイトは、1次サイトであるコンテンツ・ホスティング・サイト111に対する需要が最大容量に近づいた時にシステムに追加される。
【0275】IX. 電子ディジタル・コンテンツ商店A. 概要 複数の電子ディジタル・コンテンツ商店103のサポート電子ディジタル・コンテンツ商店103は、本質的に小売業者である。これは、コンテンツ113を市場で売って顧客に配布する実体である。コンテンツ113の配布に関して、これには、ディジタル・コンテンツ小売りウェブ・サイト、ディジタル・コンテンツ小売り商店、または電子的なコンテンツ113を顧客に売ることにかかわることを望む会社が含まれるはずである。これらの会社は、電子的なコンテンツ113だけの販売を行うことができ、また、現在販売用に提供している他の商品が何であれ、それに電子商品の販売を追加することを選択することができる。電子ディジタル・コンテンツ商店103のサービス・オファリングへのダウンロード可能電子商品の導入は、セキュア・ディジタル・コンテンツ電子配布システム100の一部として電子ディジタル・コンテンツ商店103用に開発されたツールの組を介して達成される。
【0276】これらのツールは、下記を行うために電子ディジタル・コンテンツ商店103によって使用される。
・コンテンツ・プロバイダ101によってパッケージ化されたメタデータSC620の獲得・サービス・オファリング作成への入力として使用するための、これらのSCからのコンテンツ113の抽出・販売用に提供しているダウンロード可能なコンテンツ113を記述したオファーSC641の作成・トランザクションSC640を作成し、エンドユーザ装置109に送信することによる販売の確認およびダウンロードの開始の処理・ダウンロード可能なコンテンツ113の販売のトランザクション・ログおよび各ダウンロードの状況の管理・状況通知およびトランザクション認証要求の処理・会計調整の実行【0277】これらのツールは、電子ディジタル・コンテンツ商店103がダウンロード可能な電子的なコンテンツ113の販売をそのサービスに統合する方法での柔軟性を可能にするように設計されている。ツールは、これが必要ではないが、購入されたダウンロード可能なコンテンツ113に関する会計清算のすべてがクリアリングハウス105によって処理されることを必要とする形で使用することができる。これらのツールは、電子ディジタル・コンテンツ商店103が、顧客に完全にサービスし、販売促進および特価提供を含む会計トランザクションをそれ自体で処理することも可能にする。これらのツールは、電子ディジタル・コンテンツ商店103が、その既存のサービスにダウンロード可能なコンテンツ113の販売をすばやく統合できるようにする。さらに、電子ディジタル・コンテンツ商店103は、ダウンロード可能なコンテンツ113をホストする必要がなく、その分散を管理する必要がない。この機能は、コンテンツ・プロバイダ101によって選択されたコンテンツ・ホスティング・サイト111によって実行される。
【0278】電子ディジタル・コンテンツ商店103用のツールは、好ましい実施形態ではJavaで実施されるが、C／C＋＋、アセンブラ、および同等物などの他のプログラミング言語を使用することができる。電子ディジタル・コンテンツ商店103用の下で説明するツールは、さまざまなハードウェア・プラットホームおよびソフトウェア・プラットホームで稼動することができることを理解されたい。完全なシステムとしてまたはその構成コンポーネントのいずれかとしての電子ディジタル・コンテンツ商店103は、ウェブなどの電子配布、またはフロッピ・ディスケット、CD－ROM、および取外し可能ハード・ディスク装置を含むがこれらに制限されないコンピュータ可読媒体内のアプリケーション・プログラムとして配布することができる。
【0279】もう1つの実施形態では、電子ディジタル・コンテンツ商店103のコンポーネントは、プログラマーズ・ソフトウェア・ツール

キットの一部である。このツールキットは、汎用の電子ディジタル・コンテンツ商店103のコンポーネントおよび下で説明するツールのコンポーネントへの定義済みのインターフェースを使用可能にする。これらの定義済みのインターフェースは、APIまたはアプリケーション・プログラミング・インターフェースの形である。これらのAPIを使用する開発者は、高水準アプリケーション・プログラムからコンポーネントの機能性のどれでも実施することができる。これらのコンポーネントへのAPIを提供することによって、プログラマが、これらのコンポーネントの機能およびリソースを再作成する必要なしに、カスタマイズされた電子ディジタル・コンテンツ商店103をすばやく開発できる。

【0280】電子ディジタル・コンテンツ商店103は、ウェブ・ベースのサービス・オファリングに制限されない。提供されるツールは、ダウンロード可能な電子的なコンテンツ113のエンドユーザへの配布に使用される伝送インフラストラクチャまたは配布モードに無関係に、このコンテンツ113の販売を希望するすべての電子ディジタル・コンテンツ商店103によって使用される。衛星インフラストラクチャおよびケーブル・インフラストラクチャを介して提供されるブロードキャスト・サービスでも、この同一のツールを使用して、電子的なコンテンツ113の獲得、パッケージ化、およびその販売の追跡が行われる。販売用の電子商品の提示と、これらのオファーをエンドユーザに配布する方法が、ブロードキャスト・ベース・サービス・オファリングと、2地点間対話式ウェブ・サービス型オファリングの間の主要な変形である。

【0281】B. 2地点間電子ディジタル・コンテンツ配布サービス2地点間とは、主に、電子ディジタル・コンテンツ商店103とエンドユーザ装置109の間の1対1対話サービスを意味する。これは、通常は、電話モデム接続またはケーブル・モデム接続を介して提供されるインターネット・ウェブ・ベースのサービスを表す。インターネット以外のネットワークも、ウェブ・サーバ／クライアント・ブラウザ・モデルに従う限り、このモデルでサポートされる。図12は、電子ディジタル・コンテンツ商店103の主要なツール、コンポーネント、および処理を示すブロック図である。

【0282】1. 統合要件セキュア・ディジタル・コンテンツ電子配布システム100は、新しいオンライン・ビジネスを創り出すだけではなく、既存の会社が現在の在庫にダウンロード可能な電子的なコンテンツ113の販売を統合するための方法を提供する。電子ディジタル・コンテンツ商店103に供給されるツールの組は、この統合作業を簡単にする。コンテンツ獲得ツール171およびSCパッカー・ツール153は、電子ディジタル・コンテンツ商店103が、参加しているコンテンツ・プロバイダ101から販売のために入手可能なものに関する情報を獲得し、電子ディジタル・コンテンツ商店自体の在庫の項目としてこれらのダウンロード可能なオブジェクトを参照するのに必要なファイルを作成するための方法を提供する。この処理は、バッチ駆動であり、大幅に自動化することができ、新しいコンテンツ113をサイトに統合するためにのみ実行される。

【0283】セキュア・ディジタル・コンテンツ電子配布用のツールは、電子的なダウンロード可能なコンテンツ113の販売をウェブ・ベースの電子ディジタル・コンテンツ商店103の通常の実施形態（すなわち、Columbia House online、Music Boulevard、@Tower）および同等物に、現在のコンテンツ113小売りパラダイムに対する最小限の変更で統合できるように設計された。統合の複数の方法が可能であり、好ましい実施形態では、電子ディジタル・コンテンツ商店103は、全製品の検索、プレビュー、選択（ショッピング・カート）、および購入のサポートを提供する。各電子ディジタル・コンテンツ商店103は、現在と同様に、その顧客と顧客ロイヤリティを確立し、それ自体のインセンティブを提供し続け、製品を市場に出す。セキュア・ディジタル・コンテンツ電子配布システム100では、在庫のどの製品が、電子ダウンロード用に使用可能でもあるかを示し、顧客が購入選択を行う時に電子ダウンロード・オプションを選択できるようにする必要だけが生じるはずである。もう1つの実施形態では、顧客のショッピング・カートに、電子媒体選択物（コンテンツ113）および物理媒体選択物の混合を含めることができる。顧客がチェック・アウトし、電子ディジタル・コンテンツ商店103が、会計清算を完了し、購入された物理的商品の出荷機能およびハンドリング機能をログ記録または通知した後に、電子ディジタル・コンテンツ商店103の商取引ハンドリング機能が、トランザクション・プロセッサ・モジュール175を呼び出して、すべての電子ダウンロードを処理させる。商取引ハンドリング機能は、単純に必要な情報を渡し、その時点からのすべての処理は、セキュア・ディジタル・コンテンツ電子配布システム100用のツールセットによって処理される。もう1つの実施形態では、電子ディジタル・コンテンツ商店103がダウンロード可能な商品だけを販売したい場合または物理的商品とダウンロード可能商品の会計清算を分離したい場合に、セキュア・ディジタル・コンテンツ電子配布システム100用のツールセットを使用して会計清算を処理するための、トランザクション処理の他の方法も可能である。

【0284】商品のダウンロードを処理するために、電子ディジタル・コンテンツ商店103は、コンテンツ・プロバイダ101のコンテンツ販売促進ウェブ・サイト156から獲得するダウンロード可能な製品ごとに製品ID（図示せず）を与えられる。この製品IDは、ダウンロード可能製品に対する顧客の購入選択に関連する。製品IDは、ユーザが購入した製品を識別するために電子ディジタル・コンテンツ商店103がトランザクション・プロセッサ・モジュール175に渡すものである。製品を記述するために作成されたSC（オファーSC641）は、これらのオブジェクトの管理を簡単にし、電子ディジタル・コンテンツ商店103にとってそれらの存在を透過的にするために、電子ディジタル・コンテンツ商店103から分離され、オファー・データベース181で保持される。

【0285】トランザクション・プロセッサ・モジュール175および他の追加機能は、ウェブ・サーバ側実行可能物（すなわち、CGI、およびNSAPI、ISAPI呼出し可能間数）として、または、単にDLLまたはCオブジェクト・ライブラリ内のAPIとして提供される。これらの機能は、エンドユーザ対話および任意選択のクリアリングハウス105との対話のための実行時処理を処理する。これらの機能は、ウェブ・サーバの商取引サービスと対話して、コンテンツ113のダウンロード処理を開始するのに必要なファイルを作成し、エンドユーザ装置109にダウンロードする。これらの機能は、許可を与え、活動の完了の通知を受け入れるための任意選択の対話も処理する。

【0286】会計調整ツール179も、電子ディジタル・コンテンツ商店103がクリアリングハウス105に連絡して、それ自体およびクリアリングハウス105のトランザクション・ログに基づいて会計を調整するのを支援するために提供される。

【0287】2. コンテンツ獲得ツール171コンテンツ獲得ツール171は、コンテンツ販売促進ウェブ・サイト156とインターフェースして、メタデータSC620のプレビューおよびダウンロードを行う責任を負う。コンテンツ販売促進サイトは、標準的なウェブ・サイトであるから、電子ディジタル・コンテンツ商店103は、ウェブ・ブラウザを使用してこのサイトをナビゲートする。ナビゲーション機能は、コンテンツ・プロバイダ101のサイト設計に基づいて変化する。販売促進情報の多数の画面を有する、広範囲の検索機能を提供するサイトがあり、タイトル、演奏者、または新リリースのリストから選択する単純なブラウザ・インターフェースを有するサイトもある。すべてのサイトに、曲またはアルバムの販売促進情報および記述的情報のすべてを含むメタデータSC620の選択が含まれる。

【0288】代替案では、電子ディジタル・コンテンツ商店103は、コンテンツ更新に加入し、FTPを介して自動的に更新を受信することができる。

【0289】メタデータの表示コンテンツ獲得ツール171は、コンテンツ販売促進ウェブ・サイト156でメタデータSC620のリンクが選択された時に必ず起動する、ウェブ・ブラウザ・ヘルパ・アプリケーションである。SCの選択は、そのSCの電子ディジタル・コンテンツ商店103へのダウンロードと、ヘルパ・アプリケーションの起動を引き起こす。コンテンツ獲得ツール171は、メタデータSC620をオープンし、それに含まれる暗号化されていない情報を表示する。表示される情報には、抽出されたメタデータ173、音楽の例の場合、曲に関連するグラフィック・イメージおよび曲を記述した情報が含まれ、メタデータSC620に含まれる場合には曲のプレビュー・クリップを聞くこともできる。コンテンツ113が音楽である場合の例では、コンテンツ・プロバイダ101によって供給される場合に、曲またはアルバムに関する販売促進情報、アルバムのタイトル、およびアーティストも表示される。この情報は、ブラウザ・ウィンドウ内で一連のリンクされたHTMLページとして表示される。曲および歌詞などの購入可能なコンテンツ113と、コンテンツ・プロ

バイダ101が保護を望む他のすべてのメタデータは、小売りコンテンツ・ウェブ・サイト180からアクセス可能にされない。
【0290】もう1つの実施形態では、コンテンツ・プロバイダ101が、任意選択の販売促進コンテンツを有料で提供する。この実施形態では、そのような販売促進コンテンツが、メタデータSC620内で暗号化される。このデータをオープンするための会計清算は、クリアリングハウス105を介して処理することができ、電子ディジタル・コンテンツ商店103の口座に、指定された料金が請求される。
【0291】メタデータの抽出プレビュー機能のほかに、このツールは、2つの追加機能すなわち、メタデータの抽出およびオファーSC641の準備を提供する。メタデータ抽出オプションを選択すると、電子ディジタル・コンテンツ商店103は、メタデータを格納するパスおよびファイル名を入力するように促される。グラフィックスおよびオーディオ・プレビュー・クリップなどの2進メタデータは、別のファイルとして格納される。テキスト・メタデータは、ASCII区切りテキスト・ファイルに格納され、小売りコンテンツ・ウェブ・サイト180は、このファイルをそのデータベースにインポートすることができる。ASCII区切りファイルのレイアウトを記述したテーブルも、別のTOCファイル内に作成される。他の各国語サポート(NLS)がサポートするフォーマットへの抽出を可能にする追加オプションが使用可能である。
【0292】抽出されたデータで供給される情報の重要な部分が、製品IDである。この製品IDは、電子ディジタル・コンテンツ商店103用の商取引ハンドリング機能が、トランザクション・プロセッサ・モジュール175(詳細についてはトランザクション処理の節を参照されたい)に対してユーザが購入したコンテンツ113を識別するために必要とするものである。トランザクション・プロセッサ・モジュール175は、この製品IDを使用して、エンドユーザ装置109への後続のダウンロードのためにオファー・データベース181から適当なオファーSC641を正しく取り出す。電子ディジタル・コンテンツ商店103は、そのサイトでダウンロード可能なコンテンツ113のオファーをどのように提示するかを完全に制御できる。電子ディジタル・コンテンツ商店103は、提供されるコンテンツ113の、この製品IDへの相互参照を保存して、セキュア・ディジタル・コンテンツ電子配布システム100用のツールと正しくインターフェースするだけでよい。この情報をここで提供することによって、電子ディジタル・コンテンツ商店103は、オファーSC641作成処理と並列に、この製品またはコンテンツ113をその在庫ページおよび販売ページ(データベース)に統合できるようになる。というのは、この両方の処理で、製品の参照に同一の製品IDが使用されるからである。これを、下でさらに説明する。
【0293】オファーSC用のSCパッカー・ツール153電子ディジタル・コンテンツ商店103は、販売するダウンロード可能なコンテンツ113を記述したオファーSC641を作成する必要がある。オファーSC641に書き込まれる情報の大半は、メタデータSC620から導出される。コンテンツ獲得ツール171は、下記によってオファーSC641を作成する。
・メタデータSC620のオファーSCテンプレートによる定義に従い、メタデータSC620から、オファーSC641に含める必要がない部分を除去する・電子ディジタル・コンテンツ商店103についてこのツールの構成オプションによって指定されるデフォルトによる定義に従って必要な追加部分を追加する・メタデータSC620のオファーSCテンプレートの定義に従って、追加の必要な入力または選択を促す・SCパッカー・ツール153を呼び出して、この情報をSCフォーマットにパックする【0294】エンドユーザ装置109のプレイヤ・アプリケーション195(下で詳細に説明する)によって表示されるメタデータは、メタデータSC620内に保持される。電子ディジタル・コンテンツ商店103のウェブ・サービス・データベースへの入力として電子ディジタル・コンテンツ商店103によってのみ使用された他の販売促進メタデータは、メタデータSC620から除去される。ウォーターマーキング命令、暗号化された対称鍵623、およびオブジェクトの許可される使用を定義する使用条件517などの、コンテンツ・プロバイダ101によって供給された権利管理情報も、保存される。
【0295】このはぎとられたメタデータSC620が、オファーSC641に含められる。電子ディジタル・コンテンツ商店103は、商店使用条件519と称するそれ自体の使用条件または購入オプションもオファーSC641に付加する。これは、対話的にまたはデフォルトの組を介して自動的に達成することができる。対話的に処理されるように構成された場合には、電子ディジタル・コンテンツ商店103は、コンテンツ・プロバイダ101によって定義された許可されるオブジェクトの使用条件517の組を示される。電子ディジタル・コンテンツ商店103は、その顧客に提供したいオプションを選択する。これらが、新しい使用条件または商店使用条件519になる。自動的に処理するためには、電子ディジタル・コンテンツ商店103は、すべてのコンテンツ113について提供されるデフォルト購入オプションの組を構成する。これらのデフォルト・オプションは、コンテンツ・プロバイダ101によって定義された許可される使用条件517に対して自動的に検査され、矛盾がない場合にはオファーSC641にセットされる。
【0296】オファーSC641が作成された後に、オファーSC641は、オファー・データベース181に格納され、メタデータSC620内で事前に割り当てられた製品IDを用いてインデクシングされる。この製品IDは、後に、オファー・データベース181とインターフェースしてパッケージ化およびエンドユーザへの送信のためにオファーSC641を取り出す時に、顧客が購入したダウンロード可能なコンテンツ113を識別するために、電子ディジタル・コンテンツ商店103によって使用される。詳細については、トランザクション・プロセッサ・モジュール175の節を参照されたい。
【0297】もう1つの実施形態では、電子ディジタル・コンテンツ商店103が、そのサイトでコンテンツSC630をホストする。この実施形態では、コンテンツ・ホスティング・サイト111のURLを電子ディジタル・コンテンツ商店103のURLに置換するなどのオファーSC641に対する変更が必要である。
【0298】3. トランザクション処理モジュール175電子ディジタル・コンテンツ商店103は、請求をクリアリングハウス105に送信する。代替案では、電子ディジタル・コンテンツ商店103は、クリアリングハウス105に直接に会計決済を要求することができる。ダウンロード可能なコンテンツ113に関するエンドユーザ購入要求の処理には、2つの基本モードがある。電子ディジタル・コンテンツ商店103が、購入の会計清算を処理することを望まず、商品の販売を左右する特別な販売促進またはインセンティブを持たず、購入要求をバッチ化するためのショッピング・カート・メタファを使用しない場合には、電子ディジタル・コンテンツ商店103は、そのコンテンツ113のダウンロード・ページにオファーSC641ファイルへの直接のリンクを設けることを選ぶことができる。オファーSC641は、メタデータ内に小売り価格決定情報が含まれる状態で作成されていなければならないはずである。やはりオファーSC641に含まれるのが、販売の期間および条件を伴う購入オプションを表す特別なHTMLオファー・ページである。このページは、オファーSC641が作成される時に作成されるテンプレートから作成される。エンドユーザが、オファーSC641への直接リンクをクリックした時に、オファーSC641がブラウザにダウンロードされ、エンドユーザ装置109がヘルパ・アプリケーションを起動し、ヘルパ・アプリケーションが、そのコンテナをオープンし、オファーSC641に含まれるオファー・ページを提示する。このページには、クレジット・カード情報および購入オプション選択を含む顧客情報を集めるためのフォームが含まれる。このフォームは、その後、会計清算および処理のためにクリアリングハウス105に直接にサブミットされる。任意選択として、このフォームに、エンドユーザの信用情報を使用するために必要なフィールド、または業界標準のローカル・トランザクション・ハンドラを含めることができる。
【0299】電子ディジタル・コンテンツ商店103が請求を処理する実施形態をこれから説明する。購入要求を処理する、より典型的なモードは、電子ディジタル・コンテンツ商店103が、会計清算を処理でき、その後、ダウンロード許可をエンドユーザにサブミットできるようにすることである。この方法では、電子ディジタル・コンテンツ商店103が、ダウンロード可能なコンテンツ113の販売をそのサイトで販売用に提供する他の商品と統合することができ、ダウンロード要求ごとの個々の料金ではなく、顧客に対する1つだけの連結された請求を伴う購入要求のバッチ処理(ショッピング・カート・メタファ)が可能になり、電子ディジタル・コンテンツ商店103が、顧客の購入パターンを直接に追跡し、特別な販売促進およびクラブ・オプションを提供することができるようになる。この環境では、ダウンロード可能なコンテンツ113の提供は、電子ディジタル・コンテンツ商店103のショッピング・ページに含まれ、電子ディジタル・コンテンツ商店103の現在のショッピング・モデルで行われているように、コンテンツは、エンドユーザによって選択された

時にショッピング・カートに追加され、処理され、会計清算される。会計清算が完了した後に、セキュア・ディジタル・コンテンツ電子配布システム100の商取引ハンドリング処理が、トランザクション・プロセッサ・モジュール175を呼び出してトランザクションを完了する。
【0300】トランザクション・プロセッサ・モジュール175トランザクション・プロセッサ・モジュール175の役割は、購入されたコンテンツ113のダウンロードを開始し、処理するためにエンドユーザ装置109が必要とする情報を集めることである。この情報は、トランザクションSC640にパッケージ化され、このトランザクションSC640は、購入サブミッションに対する応答としてウェブ・サーバによってエンドユーザ装置109に送り返される。トランザクション・プロセッサ・モジュール175は、電子ディジタル・コンテンツ商店103の商取引ハンドリング処理からの3つの情報すなわち、購入されたコンテンツ113の製品ID、トランザクション・データ642、および購入清算を確認するHTMLページまたはCGI URLを必要とする。
【0301】製品IDは、販売されたコンテンツ113に関連するメタデータSC620内で電子ディジタル・コンテンツ商店103に供給される値である。この製品IDは、オファー・データベース181から関連するオファーSC641を取り出すのに使用される。
【0302】トランザクション・データ642は、電子ディジタル・コンテンツ商店103のトランザクション処理機能によって提供される情報の構造であり、これは、後に、クリアリングハウス105の処理を電子ディジタル・コンテンツ商店103によって実行された会計清算トランザクションと相関させ、エンドユーザ装置109にダウンロードされるコンテンツ113の透かしに含まれるユーザ識別情報を供給するのに使用される。クリアリングハウス105は、注文SC650を受信した時に、トランザクションをログ記録して、販売されたコンテンツ113、それを販売した電子ディジタル・コンテンツ商店103、およびエンドユーザの名前とトランザクションID535を含む関連するトランザクション・データ642を示す。トランザクションID535は、会計清算トランザクションへの参照を提供する。この情報は、後に、電子ディジタル・コンテンツ商店103がその口座をコンテンツ・プロバイダ101（またはその代理人）から受け取った請求計算書と調整するのに使用するために、クリアリングハウス105によって電子ディジタル・コンテンツ商店103に返される。クリアリングハウスのトランザクション・ログ178は、コンテンツ・プロバイダ101によって、どのコンテンツ113が販売されたかを判定し、それが所有する使用料について各電子ディジタル・コンテンツ商店103への請求書を作成できるようにするのに使用することができる。請求以外の他の電子的手段をその代わりに使用して、コンテンツ・プロバイダ101と電子ディジタル・コンテンツ商店103の間で口座の清算を行うことができる。
【0303】トランザクションSC640内で供給される情報と、トランザクションSC640のセキュリティおよび保全性は、購入トランザクションが有効であり、したがって、クリアリングハウス105によるこの販売のログ記録の前にこれ以上の検証が不要であることの、クリアリングハウス105に対する十分な認証性をもたらす。しかし、電子ディジタル・コンテンツ商店103は、その口座に請求される（この電子ディジタル・コンテンツ商店103がこのコンテンツ113の販売の代金を集めたことをコンテンツ・プロバイダ101に示すクリアリングハウス105でログ記録されるトランザクションの）前に、認証を要求するオプションを有する。この認証／通知の要求は、トランザクション・データ642のフラグによって示される。このシナリオでは、クリアリングハウス105が、電子ディジタル・コンテンツ商店103に連絡し、その口座への請求および対称鍵623の公開の前に、電子ディジタル・コンテンツ商店103から許可を受信する。トランザクションID535が、この認証要求の一部としてクリアリングハウス105から電子ディジタル・コンテンツ商店103に渡されて、電子ディジタル・コンテンツ商店103が、この要求を、エンドユーザについて実行された前のトランザクションに関連付けることができるようになる。このトランザクションID535は、電子ディジタル・コンテンツ商店103が使用したい任意の一意の値とすることができ、電子ディジタル・コンテンツ商店103だけのためのものである。
【0304】トランザクション・データ642には、顧客の名前も含まれる。この名前は、購入時にユーザが書き込む購入フォームのユーザ名フィールドからとるか、以前に電子ディジタル・コンテンツ商店103へのユーザ登録処理中にログ記録された情報からとるか、このトランザクションに使用されるカードに関連するクレジット・カード情報から得た公式の名前とすることができる。この名前は、後に、ライセンス透かし527に含められる。
【0305】トランザクション・データ642には、エンドユーザによって購入された商店使用条件519も含まれる。この情報は、ライセンス透かし527に含まれ、エンドユーザ装置109によってコピーおよび再生制御に使用される。
【0306】トランザクション・プロセッサ・モジュール175が必要とする最後のパラメータは、購入清算を確認するHTMLページまたはCGI URLである。これの目的は、電子ディジタル・コンテンツ商店103が、会計清算の確認および応答に含めたい他の情報をエンドユーザに返すことができるようにすることである。このHTMLページまたはCGI URLは、トランザクションSC640に含まれ、トランザクションSC640が受信され、処理される時に、エンドユーザ装置109のブラウザ・ウィンドウに表示される。
【0307】トランザクションSC640は、購入サブミッションを処理した後の電子ディジタル・コンテンツ商店103からエンドユーザへのHTTP応答である。直接HTTP応答としてSCを送信することによって、エンドユーザ装置109上でのSCプロセッサ・ヘルパ・アプリケーションの自動ローディングが強制され、したがって、その後のエンドユーザが開始する活動に依存せずに、トランザクションを自動的に完了できるようになる。この処理を、エンドユーザ装置109およびプレイヤ・アプリケーション195の節で詳細に説明する。
【0308】トランザクション・プロセッサ・モジュール175は、必要なパラメータを用いて呼び出された時に、トランザクション・データ642、トランザクション確認HTMLページまたは参照URLおよびSCの他の必要なセキュリティ特徴を含むトランザクションSC640を作成し、購入に関連するオファーSC641を取り出し、埋め込む。トランザクション・プロセッサ・モジュール175は、通知インターフェース・モジュール176および会計調整ツール179による後の使用のためにこのトランザクションに関する情報もログ記録する。
【0309】4. 通知インターフェース・モジュール176通知インターフェース・モジュール176は、ウェブ・サーバ側実行可能ルーチン（CGIか、NSAPI、ISAPI、または同等物によって呼出し可能な関数）である。通知インターフェース・モジュール176は、クリアリングハウス105、エンドユーザ装置109、コンテンツ・ホスティング・サイト111、およびコンテンツ・プロバイダ101からの任意選択の要求および通知を処理する。電子ディジタル・コンテンツ商店103が任意選択として通知を要求することができるイベントは次の通りである。
・エンドユーザ装置109が暗号化鍵623を要求し、クリアリングハウス105が指定されたコンテンツ113の暗号化鍵623を公開しようとしていることの、クリアリングハウス105からの通知。この通知は、任意選択として、暗号化鍵623をエンドユーザ装置109に送信する前に、電子ディジタル・コンテンツ商店103からの認証を必要とするように構成することができる。
・コンテンツSC630がエンドユーザ装置109に送信されたことの、コンテンツ・ホスティング・サイト111からの通知。
・コンテンツSC630およびライセンスSC660が受信され、コンテンツ113の処理に成功裡に使用されたか、壊れていることがわかったことの、エンドユーザ装置109からの通知。
・新しいコンテンツ113がコンテンツ販売促進ウェブ・サイト156に配置されたことの、コンテンツ・プロバイダ101からの通知。
【0310】これらの通知のどれもが、セキュア・ディジタル・コンテンツ電子配布システム100の必要なステップではないが、電子ディジタル・コンテンツ商店103が、販売の完了の満足に関するレコードをクローズする機会を得られるようにするために、オプションとして提供される。これらの通知は、トランザクションの会計清算以降に発生した機能または販売完了の試みの間に発生したエラーを電子ディジタル・コンテンツ商店103に知らせることによって、顧客サービス要求を処理するのに必要になる可能性がある情報も提供する。その代わりに、この状況の大半を、必要に応じて顧客サービス・インターフェース184を介してクリアリングハウス105から得ることができる。
【0311】コンテンツ販売促進ウェブ・サイト156で使用可能な新しいコンテンツ113の通知の頻度は、コンテンツ・プロバイダ101によって決定される。通知は、新しいメタデータSC620が追加されるたびに、または毎日、その日に追加されたすべての新しいメ

タデータSC620について、供給することができる。
【0312】これらの通知のすべてが、トランザクション・ログ178への項目の作成をもたらす。電子ディジタル・コンテンツ商店103は、これらの通知に対するそれ自体の処理を実行したい場合に、CGI呼出しをインターセプトし、独自の機能を実行し、その後、任意選択として要求を通知インターフェース・モジュール176に渡すことができる。
【0313】5. 会計調整ツール179この会計調整ツール179は、クリアリングハウス105に連絡して、トランザクション・ログ178とクリアリングハウス105のログを比較する。これは、電子ディジタル・コンテンツ商店103がセキュア・ディジタル・コンテンツ電子配布システム100の会計について気持ちよく感じるのを助けるために使用可能な任意選択の処理である。
【0314】もう1つの実施形態では、このツールを更新して、コンテンツ・プロバイダ101およびクリアリングハウス105への自動化された定期的支払のための電子資金移動を提供することができる。このツールは、クリアリングハウス105から電子請求書を受信した時に、トランザクション・ログ178に対して請求書を調整した後に支払を自動的に処理するように設計することもできる。
【0315】C. ブロードキャスト電子ディジタル・コンテンツ配布サービスブロードキャストとは、主に、オンデマンドの視聴をカスタマイズするためのエンドユーザ装置109と電子ディジタル・コンテンツ商店103の間の個人的対話がない、1対多伝送方法を指す。これは、通常は、コンテンツ113が事前にプログラムされ、その結果、すべてのエンドユーザ装置109が同一のストリームを受信する、ディジタル衛星インフラストラクチャまたはケーブル・インフラストラクチャを介して提供される。
【0316】電子ディジタル・コンテンツ商店103が、サイト設計に大量の共通性を有する、インターネット接続を介するウェブ配布インターフェースならびにブロードキャスト・サービスを介する高帯域幅の衛星またはケーブル配布インターフェースの両方を提供できるような形で編成されたディジタル・コンテンツ・サービスを提供する、ハイブリッド・モデルを定義することもできる。IRDバックチャネル・シリアル・インターフェースがウェブに接続され、IRDがウェブ・ナビゲーションをサポートする場合、エンドユーザは、バックチャネル・インターネット・インターフェースを介して通常の形でディジタル・コンテンツ・サービスをナビゲートし、購入するコンテンツ113のプレビューと選択を行うことができる。ユーザは、すべてインターネット接続を介して、高品質のダウンロード可能なコンテンツ113を選択し、これらの選択物を購入し、必要なライセンスSC660を受信することができ、その後、高帯域幅ブロードキャスト・インターフェースを介してコンテンツ113(コンテンツSC630)の配布を要求することができる。ウェブ・サービスは、ブロードキャスト・スケジュールに基づいて、この形でダウンロードするために使用可能なコンテンツ113を示すか、購入されたコンテンツ113に完全に基づいてブロードキャスト・ストリームを作成することができる。この方法では、ウェブ・ベースのディジタル・コンテンツ・サービスが、ブロードキャスト施設と契約して、正しい機器を持つユーザに高品質のコンテンツ113を配布できるようになり、限られた数の特定のコンテンツ113(たとえば曲またはCD)を毎日この形で入手できるようにし、カタログ全体を低品質でウェブ・インターフェース経由でダウンロードのために使用可能にすることができる。
【0317】エンドユーザ装置109へのウェブ・インターフェースがない、他のブロードキャスト・モデルを設計することができる。このモデルでは、販売促進コンテンツは、エンドユーザ装置109(すなわちIRD)へのブロードキャスト配布のための特別なフォーマットのディジタル・ストリームにパッケージ化され、エンドユーザ装置109で特別な処理を実行して、ストリームを復号し、販売促進コンテンツをエンドユーザに提示し、そこから購入選択を行えるようにする。
【0318】実際の購入選択は、まだエンドユーザ装置109からクリアリングハウス105へのバックチャネル通信を介して開始され、SCを使用してすべてのデータ交換が実行されるはずである。電子ディジタル・コンテンツ商店103に供給されるツールセットは、ほとんどのツールが2地点間インターネット・サービス・オファリングならびにブロードキャスト衛星オファリングまたはブロードキャスト・ケーブル・オファリングの両方に適用される形で設計され、開発されている。電子ディジタル・コンテンツ商店103のディジタル・コンテンツ・ウェブ・サイトで、コンテンツ113の獲得および管理ならびにSCの準備に使用されるツールは、衛星ベースの電子ディジタル・コンテンツ商店103によって、ブロードキャスト・インフラストラクチャでの配布のためのコンテンツ113の管理および準備にも使用される。ウェブ・サービスを介して配布されるSCは、ブロードキャスト・サービスを介して配布されるSCと同一である。
【0319】X. エンドユーザ装置109セキュア・ディジタル・コンテンツ電子配布システム100用のエンドユーザ装置109のアプリケーションは、2つの主要な機能すなわち、第1にSC処理およびコピー制御、第2に暗号化されたコンテンツ113の再生を実行する。エンドユーザ装置109は、パーソナル・コンピュータであっても特殊化された電子消費者装置であっても、これらの基本機能を実行できなければならない。エンドユーザ装置109は、再生リストの作成、ディジタル・コンテンツ・ライブラリの管理、コンテンツ再生中の情報およびイメージの表示、外部媒体装置へのレコーディングなどのさまざまな追加の特徴および機能も提供する。これらの機能は、これらのアプリケーションがサポートするサービスと、アプリケーションが設計された対象の装置の種類に基づいて変化する。
【0320】A. 概要ここで図13を参照すると、主要なコンポーネントおよび処理とエンドユーザ装置109の機能フローが示されている。PCベースのウェブ・インターフェースのコンテンツ113のサービスをサポートするように設計されたアプリケーションは、2つの実行可能ソフトウェア・アプリケーションすなわち、SCプロセッサ192およびプレイヤ・アプリケーション195からなる。SCプロセッサ192は、SCファイル／MIMEタイプを処理するための、エンドユーザ・ウェブ・ブラウザ191へのヘルパ・アプリケーションとして構成された実行可能アプリケーションである。このアプリケーションは、電子ディジタル・コンテンツ商店103、クリアリングハウス105、またはコンテンツ・ホスティング・サイト111からSCを受信した時に必ずブラウザによって起動される。このアプリケーションは、SCの必要なすべての処理を実行し、最終的に、エンドユーザのディジタル・コンテンツ・ライブラリ196にコンテンツ113を追加する責任を負う。
【0321】プレイヤ・アプリケーション195は、エンドユーザが自分のディジタル・コンテンツ・ライブラリ196内のコンテンツ113を実行し、ディジタル・コンテンツ・ライブラリ196を管理し、許可される場合にコンテンツ113のコピーを作成するためにロードする、独立の実行可能アプリケーションである。プレイヤ・アプリケーション195およびSCプロセッサ192アプリケーションの両方を、Java、C／C＋＋、または同等のソフトウェア言語で記述することができる。好ましい実施形態では、これらのアプリケーションを、ウェブサイトなどのコンピュータ可読手段からダウンロードすることができる。しかし、ディスケットまたはCDなどのコンピュータ可読媒体上で配布するなど、他の配布機構も可能である。
【0322】コンテンツ113情報の検索およびブラウジング、たとえば曲クリップのプレビュー、および購入のための曲の選択は、すべてがエンドユーザ・ウェブ・ブラウザ191を介して処理される。電子ディジタル・コンテンツ商店103は、多数のコンテンツ113小売りウェブ・サイトによって現在提供されているものと同一の形のショッピング経験を提供する。現在のウェブ・ベースのコンテンツ113ショッピングに対するエンドユーザにとっての相違は、ダウンロード可能なコンテンツ113オブジェクトを選択して自分のショッピング・カートに追加することができることである。電子ディジタル・コンテンツ商店103が、ダウンロード可能オブジェクトのほかに販売のために使用可能な他の商品を有する場合には、エンドユーザは、自分のショッピング・カートに物理的な商品と電子的なダウンロード可能商品の組合せを有することができる。セキュア・ディジタル・コンテンツ電子配布システムのエンドユーザ装置109は、エンドユーザがチェックアウトし、自分の最終的な購入許可を電子ディジタル・コンテンツ商店103にサブミットするまでは使用されない。この点から後は、すべての対話が、電子ディジタル・コンテンツ商店103のウェブ・サーバとエンドユーザ装置109のエンドユーザ・ウェブ・ブラウザ191の間で行われる。これには、サンプルのディジタル・コンテンツ・クリップのプレビューが含まれる。ディジタル・コンテンツ・クリップは、SCにパッケージ化はされないが、その代わりに、ダウンロード可能ファイルとして電子ディジタル・コンテンツ商店103のウェブ・サービスに統合化されるか、ストリーミング・サーバから供給される。コンテンツ113のクリップのフォーマットは、システム・アーキテクチャによって指定されるものではない。もう1つの実施形態では、プレイヤ・アプリケーション195が、電

子ディジタル・コンテンツ商店103またはクリアリングハウス105と直接に対話するか、販売促進CDを使用してオフラインになることができる。
【0323】B. アプリケーションのインストールプレイヤ・アプリケーション195およびヘルパ・アプリケーション198は、多数のウェブ・サイトからダウンロードのために使用可能な自己インストール式実行可能プログラムにパッケージ化される。クリアリングハウス105は、公開ウェブ・サイトでマスタ・ダウンロード・ページをホストする中心位置として働く。このサイトには、インストール・パッケージをダウンロードすることができる位置へのリンクが含まれる。ダウンロード要求の地理的分散をもたらすために、インストール・パッケージはすべてのコンテンツ・ホスティング・サイト111で入手可能である。参加する電子ディジタル・コンテンツ商店103のそれぞれも、そのサイトからのダウンロードのためにパッケージを使用可能にすることができ、クリアリングハウス105の公開ウェブ・サイトのマスタ・ダウンロード・ページへのリンクだけを設けることもできる。
【0324】ダウンロード可能なコンテンツ113の購入を希望するエンドユーザは、このパッケージをダウンロードし、インストールする。インストールは、このダウンロード可能パッケージ内で自己完結型になっている。パッケージは、ヘルパ・アプリケーション198およびプレイヤ・アプリケーション195の両方をアンパックし、インストールし、インストールされているウェブ・ブラウザに合わせてヘルパ・アプリケーション198を構成する。
【0325】インストールの一部として、公開鍵661／秘密鍵対が、注文SCおよびライセンスSC660の処理で使用するためにエンドユーザ装置109用に作成される。乱数の対称鍵（秘密ユーザ鍵）も、ライセンス・データベース197での曲暗号化鍵の保護に使用するために生成される。秘密ユーザ鍵（図示せず）は、鍵を複数の部分に分割し、鍵の各部をエンドユーザのコンピュータ全体の複数の位置に格納することによって保護される。このコードの区域は、鍵がどのようにセグメント化され、どこに格納されたかが漏れないように、耐タンパ・ソフトウェア技術を用いて保護される。エンドユーザでさえこの鍵にアクセスできなくすることが、海賊行為または他のコンピュータとのコンテンツ113の共用を防ぐのに役立つ。これらの鍵の使用方法の詳細については、SCプロセッサ192の節を参照されたい。
【0326】耐タンパ・ソフトウェア技術は、ハッカーによるコンピュータ・ソフトウェア・アプリケーションへの許可されない侵入を阻止する方法である。通常、ハッカーは、使用に対する制限を除去するために、ソフトウェアを理解し、変更することを望む。実際には、ハッキングできないコンピュータ・プログラムは存在しないので、耐タンパ・ソフトウェアは、「タンパ・プルーフ（tamper-proof）」とは呼ばれない。しかし、耐タンパ・プロテクト・アプリケーションをハッキングするのに必要な労力の量は、通常は、その労力が可能な利益に値しないので、ほとんどのハッカーを阻止する。この場合、その労力は、コンテンツ113の一部分、おそらくはCD上の1曲だけへの鍵へのアクセス権を得ることになる。
【0327】耐タンパ・ソフトウェア技術の1種が、IBMから提供されている。このコードが導入された製品の1つが、IBM ThinkPad 770ラップトップ・コンピュータである。この場合、耐タンパ・ソフトウェアは、コンピュータ内のDVDムービー・プレイヤの保護に使用された。ハリウッド・スタジオなどのディジタル・コンテンツ・プロバイダは、ディジタル・ムービーの出現と、完全なコピーを簡単に作成できることに懸念を抱き、DVDディスク上の映画にコピー・プロテクション機構を含めることを主張した。IBMの耐タンパ・ソフトウェアは、これらのコピー・プロテクション機構を迂回することを困難にする。これは、耐タンパ・ソフトウェアの非常に典型的な応用例である。このソフトウェアは、いくつかの保護されたタイプのコンテンツ113の使用に対する規則の強制に使用される。
【0328】IBMの耐タンパ・ソフトウェアは、攻撃者の通り道に複数のタイプの障害物を置く。第1に、これには、ハッカーが使用する標準的なソフトウェア・ツールすなわち、デバッガおよびアセンブラをまかすか、少なくともその有効性を減らす技法が含まれる。第2に、これには自己保全性検査が含まれ、その結果、単一の変更または少数の変更でも検出され、不正動作を引き起こす。最後に、これには、その真の動作に関してハッカーを誤った方向に導く不明瞭さが含まれる。後者の技法は、主としてその場限りであるが、最初の2つは、暗号作成術で周知のツールすなわち、暗号化およびディジタル署名に基づいて作成される。
【0329】C. SCプロセッサ192エンドユーザが、ショッピング・カートに集めた商品について電子ディジタル・コンテンツ商店103に最終購入許可をサブミットする時に、そのエンドユーザのウェブ・ブラウザは、ウェブ・サーバからの応答を待ってアクティブのままになる。電子ディジタル・コンテンツ商店103のウェブ・サーバは、購入を処理し、会計清算を実行し、その後、トランザクションSC640をエンドユーザ装置109に返す。SCプロセッサ192（ヘルパ・アプリケーション198）が、ウェブ・ブラウザによって起動されて、トランザクションSC640に関連するSC MIMEタイプを処理する。図17は、本発明による、図13に記載のようにローカル・ライブラリにコンテンツをダウンロードする、プレイヤ・アプリケーション195のユーザ・インターフェース画面の例である。
【0330】SCプロセッサ192は、トランザクションSC640をオープンし、その中に含まれる応答HTMLページおよびオファーSC641を抽出する。応答HTMLページは、ブラウザ・ウィンドウ内に表示され、エンドユーザの購入を確認する。その後、オファーSC641がオープンされ、コンテンツ113（たとえば曲またはアルバム）の名前が、予測ダウンロード時間と共にそこから抽出される（ステップ1401）。その後、この情報を含む新しいウィンドウが表示され、エンドユーザに、コンテンツ113（たとえば、音楽の場合、曲またはアルバム全体）のダウンロードをスケジューリングするオプションが提示される（ステップ1402）。エンドユーザは、即時ダウンロードを選択するか、後の時刻にダウンロードを行うようにスケジューリングすることができる。後の時刻が選択された場合、ダウンロード・スケジュール情報が、ログに保管され、スケジューリングされた時刻にエンドユーザ装置109の電源が入っている場合に、その時点でダウンロードが開始される。スケジューリングされたダウンロード時刻にコンピュータがアクティブでないか、通信リンクがアクティブでない場合には、次にコンピュータの電源を入れた時に、エンドユーザは、ダウンロードをスケジューリングしなおすように促される。
【0331】スケジューリングされたダウンロード時刻になるか、即時ダウンロードが要求された場合には、SCプロセッサ192は、トランザクションSC640、オファーSC641、およびインストール時に生成されたエンドユーザの公開鍵661の情報から注文SC650を作成する。この注文SC650が、HTTP要求を介してクリアリングハウス105に送信される。クリアリングハウス105がライセンスSC660を返した時に、ヘルパ・アプリケーション198が再び呼び出されて、ライセンスSC660を処理する。その後、ライセンスSC660がオープンされ、コンテンツ・ホスティング・サイト111のURLが、参照される注文SC650から抽出される。その後、ライセンスSC660は、ブラウザを介するHTTP要求を介して指定されたコンテンツ・ホスティング・サイト111に送信され、コンテンツSC630のダウンロードを要求する。コンテンツSC630がブラウザに返された時に、ヘルパ・アプリケーション198が再び呼び出される。SCプロセッサ192は、ダウンロード中のコンテンツ113の名前を、ダウンロード進行インジケータおよび推定完了時刻と共に表示する。
【0332】コンテンツ113がSCプロセッサ192によって受信されている間に、SCプロセッサ192は、コンテンツ113のデータを解読のためにメモリ・バッファにロードする。バッファのサイズは、暗号化アルゴリズムおよびウォーターマーキング193の要件に依存し、ハッカー・コードに露出される解読されたコンテンツ113の量を減らすために、可能な最小のサイズである。バッファは、満杯になった時に、ライセンスSC660から抽出されたエンドユーザの対称鍵623（公開鍵661に対応する）を使用して解読され、対称鍵623自体は、まず秘密鍵を使用して暗号化されている。解読されたバッファは、ウォーターマーキング機能に渡される。
【0333】ウォーターマーキング193は、ライセンスSC660からウォーターマーキング命令を抽出し、エンドユーザの秘密鍵を使用してその命令を解読する。その後、このコンテンツ113が購入された電子ディジタル・コンテンツ商店103に登録された購入者の名前または、電子ディジタル・コンテンツ商店103が登録機能を提供しない場合にはクレジット・カード登録情報から導出される購入者の名前などのトランザクション情報を含むウォーターマーキング・データが、ライセンスSC660から抽出される。透かしには、購入日および、このトランザクションについてログ記録された特定のレコードを参照するために電子ディジタル・コンテンツ商店103に

よって割り当てられたトランザクションID535も含まれる。商店使用条件519も、プレイヤ・アプリケーション195のコピー制御による使用のために含まれる。

【0334】ウォーターマーキング193は、ウォーターマーキング命令が漏れないように耐タンパ・コード技術を用いて保護され、したがって、ハッカーが透かしの位置および技法を発見できないようになっている。これによって、ハッカーによる透かしの除去または変更が防止される。

【0335】必要な透かしをこのコンテンツ・バッファに書き込んだ後に、バッファを、解読および再暗号化194のスクランブル化機能に渡す。IBMのSEAL暗号化技術などのプロセッサ効率のよいセキュア暗号化アルゴリズムを使用して、ランダムな対称鍵を使ってコンテンツ113を再暗号化する。ダウンロードと解読および再暗号化194の処理が完了した後に、コンテンツ・プロバイダ101が最初にコンテンツ113を暗号化するのに使用した暗号化鍵623が、破壊され、新しいSEAL鍵自体が、インストール時に作成され、隠された秘密ユーザ鍵を使用して暗号化される。この新たに暗号化されたSEAL鍵は、ライセンス・データベース197に格納される。

【0336】コンテンツ・プロバイダ101およびユーザで実行されるソースとは異なり、エンドユーザ装置109で実行されるユーザ・ウォーターマーキングは、業界標準が有効になることを必要とする可能性がある。これらの標準は、まだ発展中である。制御情報を音楽に埋め込み、複数回更新できるようにする技術が使用可能である。コピー制御標準規格がより安定する時まで、コピー制御の代替方法がセキュア・ディジタル・コンテンツ電子配布システム100内で提供され、その結果、このシステムは、消費者装置での権利管理を提供するためにコピー制御透かしに依存しないようになる。記憶および再生／記録使用条件のセキュリティは、エンドユーザ装置109に拘束され、耐タンパ環境を介して保護される暗号化されたディジタル・コンテンツ・ライブラリ196を使用して実施される。ソフトウェア・フックが適所にあって、標準規格が採用された時にコピー制御ウォーターマーキングをサポートする。AACおよび他の符号化されたオーディオ・ストリームにさまざまな圧縮レベルでウォーターマーキングするためのサポートが現在存在するが、この技術は、現時点では、コピー制御の唯一の方法として使用するにはまだいくぶん未成熟である。

【0337】解読および再暗号化194の処理は、元のコンテンツ113暗号化鍵と、新しいSEAL鍵と、秘密ユーザ鍵と、秘密ユーザ鍵セグメントが格納される位置および鍵をセグメント化する方法とが漏れないように耐タンパ・コード技術を用いて保護される、コードのもう1つの区域である。

【0338】解読および再暗号化194の処理は、2つの目的にかなう。SEALなどのアルゴリズムを用いて暗号化されたコンテンツ113の記憶は、リアルタイム解読より高速化が可能であり、解読を実行するために、DESなどのより業界標準型のアルゴリズムよりはるかに低いプロセッサ利用度を必要とする。これによって、プレイヤ・アプリケーション195が、復号および再生の前にまずコンテンツ113のファイル全体を解読する必要なしに、コンテンツ113のリアルタイムで並列の解読－復号－再生を実行できるようになる。SEALアルゴリズムの効率および非常に効率的な復号アルゴリズムは、並列動作（暗号化されたファイルからのストリーミング再生）を可能にするだけではなく、はるかに低い処理能力を有するプロセッサでこの処理を行えるようにもする。したがって、このアプリケーションは、60MHz Pentiumシステムおよびおそらくそれ以下のローエンドのエンドユーザ装置109でサポートできる。コンテンツ113が最終的に格納される暗号化フォーマットと元の暗号化フォーマットを分離することによって、元のコンテンツ暗号化アルゴリズムの選択でのより高い柔軟性が可能になる。したがって、広く受け入れられ、実績がある業界標準アルゴリズムを使用することができ、したがって、ディジタル・コンテンツ産業のセキュア・ディジタル・コンテンツ電子配布システム100の受入がさらに強化される。

【0339】この解読および再暗号化194の処理の第2の目的は、このコンテンツ113の暗号化にコンテンツ・プロバイダ101によって使用された元のマスタの暗号化鍵623を、このコンテンツ113のライセンスを交付されたエンドユーザ装置109のすべてに格納する必要をなくすことである。暗号化されたマスタの対称鍵623は、ライセンスSC660の一部として、非常に短い時間だけエンドユーザ装置109のハード・ディスクにキャッシュ記憶されるだけであり、平文では非常に短い時間だけメモリ内だけにある。この実行相の間に、対称鍵623は、耐タンパ・コード技術を介して保護される。この解読および再暗号化194の相が完了した後に、いかなる形でもエンドユーザ装置109にこの対称鍵623を保存する必要をなくすことによって、ハッカーからの海賊行為の可能性が大幅に低下する。

【0340】曲は、再暗号化された後に、ディジタル・コンテンツ・ライブラリ196に格納される。プレイヤ・アプリケーション195による使用のために必要なすべてのメタデータが、関連するオファーSC641から抽出され、やはりディジタル・コンテンツ・ライブラリ196に格納される（ステップ1403）。メタデータのうちで、歌詞などの暗号化された部分は、他のコンテンツについて上で説明したものと同じ形で解読され、再暗号化される。コンテンツ113の暗号化に使用されたものと同一のSEAL鍵が、暗号化を必要とする関連するメタデータに使用される。

【0341】D. プレイヤ・アプリケーション1951. 概要セキュア・ディジタル・コンテンツ電子配布システムのプレイヤ・アプリケーション195は、CDプレイヤ、DVDプレイヤ、または他のディジタル・コンテンツ・プレイヤと、CD、DVD、または他のディジタル・コンテンツ記憶管理システムの両方に類似する。最も単純なレベルでは、プレイヤ・アプリケーション195は、曲またはビデオの再生など、コンテンツ113を実行する。別のレベルでは、プレイヤ・アプリケーション195は、エンドユーザに、自分のディジタル・コンテンツ・ライブラリ196を管理するツールを提供する。同様に重要なことに、プレイヤ・アプリケーション195は、曲などのコンテンツの集合（本明細書では再生リストと称する）の編集および再生を提供する。

【0342】プレイヤ・アプリケーション195は、個別に選択し、コンテンツ・プロバイダ101および電子ディジタル・コンテンツ商店103の要件に合わせてカスタマイズすることのできるコンポーネントの集合から組み立てられる。汎用版のプレイヤを説明するが、カスタマイズが可能である。

【0343】ここで図18および19を参照すると、図13のエンドユーザ装置109で稼動するプレイヤ・アプリケーション195の主要なコンポーネントと処理のブロック図が示されている。

【0344】プレイヤ・オブジェクト・マネージャ1501のサブシステムを構成する複数のコンポーネントセットがある。

1. エンドユーザ・インターフェース・コンポーネント15092. コピー／再生管理コンポーネント15043. 解読1505、圧縮解除1506、再生コンポーネント1507、およびレコーディングを含めることができる。

4. データ管理1502およびライブラリ・アクセス・コンポーネント15035. アプリケーション間通信コンポーネント15086. その他の（インストールなど）コンポーネントこれらのセットのそれぞれからのコンポーネントを、下記の要件に基づいて選択することができる。

・プラットホーム（Windows（登録商標）、Unix、または同等物）
・通信プロトコル（ネットワーク、ケーブルなど）
・コンテンツ・プロバイダ101または電子ディジタル・コンテンツ商店103・ハードウェア（CD、DVDなど）
・クリアリングハウス105技術その他【0345】下の節で、さまざまなコンポーネント・セットを詳細に説明する。最後の節で、汎用プレイヤ内でこれらのコンポーネントを集める方法の詳細を説明し、これらのコンポーネントをカスタマイズする方法を説明する。

【0346】もう1つの実施形態では、プレイヤ・アプリケーション195およびSCプロセッサ192のコンポーネントが、プログラマーズ・ソフトウェア・ツールキットの一部として使用可能である。このツールキットは、上に一覧を示した汎用プレイヤ・アプリケーションのコンポーネントへの定義済みのインターフェースを使用可能にする。これらの定義済みのインターフェースは、APIまたはアプリケーション・プログラミング・インターフェースの形である。これらのAPIを使用する開発者は、高水準アプリケーション・プログラムからコ

ンポーネントのどの機能性でも実施することができる。これらのコンポーネントへのAPIを提供することによって、プログラマが、これらのコンポーネントの機能およびリソースを再作成する必要なしに、カスタマイズされたプレイヤ・アプリケーション195をすばやく開発できる。

【0347】2. エンドユーザ・インターフェース・コンポーネント1509このセットのコンポーネントは、プレイヤ・アプリケーション195のオンスクリーン表示を提供するために組み合わされる。設計では、これらのコンポーネントの決定的なレイアウトが確立されないことに留意されたい。そのようなレイアウトの1つが、汎用プレイヤで提供される。コンテンツ・プロバイダ101または電子ディジタル・コンテンツ商店もしくはその両方の要件および他の要件に基づいて、代替レイアウトが可能である。

【0348】このセットは、まずエンドユーザ表示1510を提示するのに使用されるコンポーネントと、オーディオ再生およびメタデータの提示などの低水準機能に使用されるエンドユーザ・コントロール1511と称するハンドル・コントロールというサブグループにグループ化される。次に、エンドユーザ表示1510は、さらに、特殊機能グループ化（再生リスト、ディジタル・コンテンツ・ライブラリ）によって分割され、その後、これらの低水準コンポーネントのグループ化および配置に使用されるオブジェクトコンテナ・コンポーネントによって分割される。

【0349】下のコンポーネント一覧内では、CDの作成またはCDもしくは他の記録可能媒体へのコンテンツ113のコピーへの言及は、プレイヤ・アプリケーション195がそのような機能性を使用可能にされている場合だけに適用される。また、その文脈での用語CDは、包括的な用語であり、ミニディスクまたはDVDなどのさまざまな他の外部記録装置も表すことができることに留意されたい。

【0350】図20は、本発明による、図18および図19のプレイヤ・アプリケーション195の例のユーザ・インターフェース画面を示す図である。エンドユーザ・コントロール1511の機能には、下記が含まれる（エンドユーザ・インターフェースの対応する画面が、符号1601ないし1605に示されている）。

【0351】コンテンツ113を実行するためのコントロール・再生／停止ボタン・再生ボタン・停止ボタン・一時停止ボタン・前のスキップ・ボタン・後ろのスキップ・ボタン・音量制御・トラック位置制御／表示・オーディオ・チャネル音量レベル表示その他。

【0352】コンテンツ113に関連するメタデータを表示するためのコントロール・カバー・ピクチャ・ボタン・カバー・ピクチャ・オブジェクト・アーティスト・ピクチャ・ボタン・アーティスト・ピクチャ・オブジェクト・トラック・リスト・ボタン・トラック・リスト情報オブジェクト・トラック・リスト・セレクタ・オブジェクト（クリックすると再生）
・トラック名オブジェクト・トラック情報オブジェクト・トラック歌詞ボタン・トラック歌詞オブジェクト・トラック・アーティスト名オブジェクト・トラック・クレジット・ボタン・トラック・クレジット・オブジェクト・CD名オブジェクト・CDクレジット・ボタン・CDクレジット・オブジェクト・汎用（構成可能）メタデータ・ボタン・汎用メタデータ・オブジェクトその他【0353】エンドユーザ表示1510の機能には、下記が含まれる（エンドユーザ・インターフェースの対応する画面が、符号1601ないし1605に示されている）

【0354】表示コンテナの再生リスト・再生リスト管理ボタン・再生リスト管理ウィンドウ・ディジタル・コンテンツ検索ボタン・ディジタル・コンテンツ検索定義オブジェクト・ディジタル・コンテンツ検索サブミット・ボタン・ディジタル・コンテンツ検索結果オブジェクト・選択された検索結果項目を再生リストにコピー・ボタン・再生リスト・オブジェクト（編集可能）
・再生リスト保存ボタン・再生リスト再生ボタン・再生リスト一時停止ボタン・再生リスト再始動ボタン・再生リストからCDを作成ボタンその他。

【0355】ディジタル・コンテンツ・ライブラリ196の表示・ディジタル・コンテンツ・ライブラリ・ボタン・ディジタル・コンテンツ・ライブラリアン・ウィンドウ・ディジタル・コンテンツ・カテゴリ・ボタン・ディジタル・コンテンツ・カテゴリ・オブジェクト・アーティスト別ボタン・ジャンル別ボタン・レーベル別ボタン・カテゴリ別ボタン・削除ボタン・再生リストに追加ボタン・CDにコピー・ボタン・曲リスト・オブジェクト・曲リスト表示コンテナその他【0356】コンテナその他・プレイヤ・ウィンドウ・コンテナ・オーディオ・コントロール・コンテナ・メタデータ・コントロール・コンテナ・メタデータ表示コンテナ・ツールバー・コンテナ・オブジェクト・サンプル・ボタン・ダウンロード・ボタン・購入ボタン・記録ボタン・プレイヤ名オブジェクト・レーベル／プロバイダ／商店広告オブジェクト・レーベル／プロバイダ／商店URLボタン・アーティストURLボタンその他【0357】3. コピー／再生管理コンポーネント1504これらのコンポーネントは、暗号化鍵のセットアップ、透かし処理、コピー管理などを処理する。クリアリングハウス105との通信、購入要求の送信その他、ペイ・パー・リスンまたはコンテンツ113への各アクセスが計上される場合などの特別なサービスのためのインターフェースも存在する。現在、クリアリングハウス105への通信の機能は、SCプロセッサ192によって処理されている。

【0358】エンドユーザ装置109でのプレイヤ・アプリケーション195によるコンテンツ113の使用は、ライセンス・データベース197などのデータベースにログ記録される。プレイヤ・アプリケーション195によるコンテンツ113の各使用の追跡を、クリアリングハウス105またはコンテンツ・プロバイダ101または電子ディジタル・コンテンツ商店103または指定され伝送インフラストラクチャ107に結合されたサイトなどの1つまたは複数のログ記録サイトに送信することができる。この送信は、使用情報をログ記録サイトにアップロードするための所定の時刻にスケジューリングすることができる。想定される所定の時刻の1つが、伝送インフラストラクチャ107が、さほどネットワーク・トラフィックで輻輳していない可能性がある早朝である。既知の技法を使用するプレイヤ・アプリケーション195が、スケジューリングされた時刻に覚醒し、ローカル・ログ記録データベースからログ記録サイトに情報を送信する。ログ記録サイトの情報を再検討することによって、コンテンツ・プロバイダ101は、コンテンツ113の人気を測定することができる。

【0359】もう1つの実施形態では、ログ記録サイトへ後でアップロードするためにコンテンツ113の使用をログ記録するのではなく、コンテンツ113の使用が、コンテンツ113の使用中にログ記録サイトにアップロードされる。たとえば、エンドユーザ装置109に記憶されたコンテンツ113の、DVDディスク、ディジタル・テープ、フラッシュ・メモリ、ミニディスク、または同等の読書可能取外し可能媒体などの外部装置への複製またはコピーの時に、その使用が、ログ記録サイトへの更新になる。これは、コンテンツ113購入時に送信される使用条件206でのコンテンツ113のコピーに対する前提条件とすることができる。これによって、コンテンツ・プロバイダ101は、コンテンツ113に対する再生、複製、または他の処置の間にコンテンツ113の使用を正確に追跡できることが保証される。

【0360】さらに、コンテンツ113に関する他の情報を、ログ記録サイトにアップロードすることができる。たとえば、コンテンツ113が実行された最後の時刻（たとえば日時）、コンテンツ113が実行された回数、コンテンツ113が、DVDディスク、ディジタル・テープ、またはミニディスクなどの許可された外部装置に複製またはコピーされたかどうかである。家族の構成員など、エンドユーザ装置109の単一のプレイヤ・アプリケーション195の複数の別個のユーザが存在する場合には、コンテンツ113のユーザの識別を、使用情報と共にログ記録サイトに送信することができる。ログ記録サイトにアップロードされた使用情報を再検討することによって、コンテンツ・プロバイダ101は、実際の使用、ユーザの識別、およびコンテンツ113が実行された回数に基づいてコンテンツ113の人気を測定することができる。実際の使用の測定によって、このシステムは、テレビジョンのニールセン視聴率方式または電話調査など、限られた数のユーザだけを1時にサンプリングし、その結果を外挿する、サンプリング方法を使用するシステムに対して、より事実駆動になる。この実施形態では、実際の使用を、電子ディジタル・コンテンツ商店103またはコンテンツ・プロバイダ101などの指定されたウェブ・サイトにログ・オンしたユーザに関する測定値とすることができる。

【0361】4. 解読1505、圧縮解除1506および再生コンポーネント1507これらのコンポーネントは、コピー／再生管理コンポーネントによって獲得された鍵を使用して、データ管理およびライブラリ・アクセス・コンポーネントから獲得したオーディオ・データのロックを解除し、適当な圧縮解除を適用して再生のためにオーディオ・データを準備し、システム・オーディオ・サービスを使用してそれを再生する。代替実施形態では、データ管理およびライブラリ・アクセス・コンポーネントから獲得したオーディオ・データを、CD、

ディスケット、テープ、またはミニディスクなどの取外し可能媒体にコピーすることができる。
【0362】5. データ管理1502およびライブラリ・アクセス・コンポーネント1503これらのコンポーネントは、エンドユーザのシステム上のさまざまな記憶装置への曲データの格納および取出ならびに格納された曲に関する情報の要求の処理に使用される。
【0363】6. アプリケーション間通信コンポーネント1508これらのコンポーネントは、セキュア・ディジタル・コンテンツ電子配布システムのプレイヤと、プレイヤ・アプリケーション195を起動する可能性があるアプリケーション(たとえばブラウザ、ヘルパ・アプリケーション、プラグインなど)またはプレイヤ・アプリケーション195がその機能を実行する時に使用を必要とする他のアプリケーションとの間の調整に使用される。たとえば、URLコントロールが活動化される時に、そのURLコントロールは、適当なブラウザを呼び出し、そのブラウザに適当なページをロードするように指示する。
【0364】7. その他種々のコンポーネント上のカテゴリに含まれない個々のコンポーネント(たとえばインストール)は、このグループに含まれる。
【0365】8. 汎用プレイヤこの節では、ある版のプレイヤ・アプリケーション195への上のコンポーネントの組合せを説明する。プレイヤ・アプリケーション195は、ソフトウェア・オブジェクトに基づくことによるカスタマイズのために設計されているので、これは、多数の可能な異なる例のうちの1つにすぎない。
【0366】プレイヤ・オブジェクト・マネージャ1501は、他のすべてのコンポーネントを一緒に保持するソフトウェア・フレームワークである。上の節で述べたように、この図でプレイヤ・オブジェクト・マネージャ1501の下にあるブロックは、どのプレイヤにも必要であるが、使用される暗号化またはスクランブル化の形式、オーディオ圧縮のタイプ、コンテンツ113のライブラリへのアクセス方法などに応じて、特殊化された版によって置換することができる。
【0367】プレイヤ・オブジェクト・マネージャ1501の上には変化するオブジェクト1512があり、これは、ほとんどは、再生または検索されるコンテンツ113に関連するメタデータから導出される。これらの変化するオブジェクトは、エンドユーザ表示1510と、エンドユーザ・コントロール1511から受け取った入力とによってエンドユーザ装置109から使用可能にされる。すべてのオブジェクトが、構成可能であり、すべてのコンテナのレイアウトが、カスタマイズ可能である。これらのオブジェクトは、C／C＋＋、Java、または他の同等のプログラミング言語で実施することができる。
【0368】プレイヤ・アプリケーション195の使い方以下の実施形態は、エンドユーザ装置109上で稼動するプレイヤ・アプリケーション195がオーディオ・プレイヤであり、コンテンツ113が音楽である場合の一例である。当業者は、他のタイプのコンテンツ113をプレイヤ・アプリケーション195によってサポートすることができることを理解されたい。通常のオーディオ愛好家は、曲を保持するCDのライブラリを有する。これらのすべてが、セキュア・ディジタル・コンテンツ電子配布システム100内で使用可能である。電子ディジタル・コンテンツ商店103から購入された曲の組は、エンドユーザのシステムのディジタル・コンテンツ・ライブラリ196内に格納される。物理的なCDに類似する曲のグループ化が、再生リストとして格納される。いくつかの場合に、再生リストは、正確にCDをエミュレートする(たとえば、市販CDのすべてのトラックが、CDのオンライン版として電子ディジタル・コンテンツ商店103から購入され、そのCDの再生リストと同等の再生リストによって定義される場合)。しかし、ほとんどの再生リストは、エンドユーザのシステムのディジタル・コンテンツ・ライブラリに格納された曲をグループ化するために、エンドユーザによって集められる。しかし、以下の議論では、用語再生リストを使用する時に、カスタム・メイドの音楽CDの例を使用する。
【0369】SCプロセッサ192アプリケーションからの呼び出しを介してプレイヤ・アプリケーション195を始動させるのではなく、エンドユーザが明示的にプレイヤ・アプリケーション195を始動する時には、プレイヤ・アプリケーション195は、最後にアクセスされた再生リストを事前にロードする。ディジタル・コンテンツ・ライブラリ196内に再生リストが存在しない場合には、再生リスト・エディタが自動的に始動される(ユーザが優先設定を介してこの機能をオフにしていない限り)。詳細については、下の再生リストの項目を参照されたい。
【0370】プレイヤ・アプリケーション195は、特定の曲を引数として呼び出すこともでき、その場合には、プレイヤ・アプリケーション195は即座に曲再生モードに入る。任意選択として、曲の再生の準備をするが、エンドユーザによる動作を待ってから進行することができる。この状況の詳細については、下の曲の再生の項目を参照されたい。
【0371】再生リスト(エンドユーザ・インターフェースの画面1603に対応する)エンドユーザが再生リスト機能を呼び出した時に、使用可能な機能は次の通りである。
・再生リストのオープン・ディジタル・コンテンツ・ライブラリアンを呼び出して、格納された再生リストのリストを選択のために表示する。詳細については下のディジタル・コンテンツ・ライブラリアンの項目も参照されたい。
・再生リストの編集・再生リスト・エディタ(下を参照)を呼び出す。再生リストがすでにロードされている場合には現在の再生リストをロードする。そうでない場合には、エディタは空の再生リストを作成する。
・再生リストの実行・曲は、選択された曲(または、曲が選択されていない場合には再生リストの先頭)から始めて、1時に1つずつ再生される。再生リスト・エディタでセットされたオプションは、再生の順序に影響する。しかし、再生リストのこの再生のオプションを変更するのに使用可能なコントロールは、ここにはない。
・曲の再生・再生リストから選択された曲だけを再生する。詳細については下の曲の再生の項目を参照されたい。
・再生リスト情報・再生リストに関する情報を表示する。
・曲情報・再生リスト内で選択されている曲に関する情報を表示する。
・ウェブ・サイト訪問・この再生リストに関連するウェブ・サイトをブラウザにロードする。
・ライブラリアン・ディジタル・コンテンツ・ライブラリアン・ウィンドウを開く。詳細については下のディジタル・コンテンツ・ライブラリアンの項目も参照されたい。
【0372】再生リスト・エディタ(エンドユーザ・インターフェースの画面1603に対応する)
再生リスト・エディタを起動した時に、エンドユーザのオプションは次の通りである。
・再生リストの表示／ロード／削除・ディジタル・コンテンツ・ライブライランが呼び出されて、ロードまたは削除する再生リストの選択のために、格納された再生リストのリストを表示する。詳細については下のディジタル・コンテンツ・ライブラリアンの項目も参照されたい。
・再生リストの保存・再生リストの現在の版をディジタル・コンテンツ・ライブラリ196に保存する。
・曲の削除・現在選択されている曲を、再生リストから削除する。
・曲の追加・ディジタル・コンテンツ・ライブラリアンが、再生リストに追加する曲の選択のために、曲検索モードで呼び出される。詳細については下のディジタル・コンテンツ・ライブラリアンの項目も参照されたい。
・曲情報の設定・再生リスト内で選択されている曲に関する情報を表示し、その情報に対する変更を可能にする。この情報は、再生リスト内に格納され、ディジタル・コンテンツ・ライブラリ196内に格納された曲に関する情報は変更されない。以下の項目を変更することができる。
・表示される曲のタイトル・曲に関するエンドユーザのメモ・曲再生時のリードイン遅延・曲再生後のフォローオン遅延・再生時の曲内の開始点・再生時の曲内の終了点・ランダム・モード用の重み付け・この曲の音量調節その他【0373】再生リスト属性設定:この再生リストの属性を表示し、それに対する変更を可能にする。以下の属性を設定することができる。
・再生リストのタイトル・再生リストのモード(ランダム、シーケンシャル、その他)
・リピート・モード(1回再生、終了時に再開、その他)

・この再生リストに関するエンドユーザのメモ【0374】ライブラリアン（エンドユーザ・インターフェースの画面1601に対応）・ディジタル・コンテンツ・ライブラリアン・ウィンドウを開く。詳細については下のディジタル・コンテンツ・ライブラリアンの項目も参照されたい。
【0375】曲の再生曲を引数としてプレイヤ・アプリケーション195を呼び出すことによるか、再生リストまたはディジタル・コンテンツ・ライブラリアン内から再生する曲を選択することのいずれかによって、再生のための曲の準備ができた時の、エンドユーザのオプションは次の通りである（エンドユーザ・インターフェースの画面1601に対応する）。
・再生・一時停止・停止・後ろへスキップ・前へスキップ・音量調節・トラック位置調節・歌詞表示・クレジット表示・CDカバー表示・アーティスト・ピクチャ表示・トラック情報の表示・他のメタデータの表示・ウェブ・サイト訪問・再生リスト・ライブラリアンその他【0376】ディジタル・コンテンツ・ライブラリアンディジタル・コンテンツ・ライブラリアンは、曲または再生リストを選択する時に暗黙のうちに呼び出す（上を参照）か、エンドユーザのシステムの曲ライブラリの管理用のそれ自体のウィンドウ内で開くことができる。その場合に、エンドユーザのオプションは次の通りである。
曲の操作：アーティスト、カテゴリ、レーベル、その他によってすべてをソートするアーティスト、カテゴリ、レーベル、その他によって曲を選択する選択した曲を現在の再生リストに追加する曲をCDにコピーする（使用可能にされている場合）
曲を削除するカテゴリに曲を追加するその他再生リストの操作：名前によってソートするカテゴリによってソートするキーワードによって検索する含まれる曲のタイトルによって検索する選択された再生リストをロードする再生リストの名前を変更する再生リストを削除する選択された再生リストからCDを作成する（使用可能にされている場合）その他【0377】図22に移ると、本発明による、コンテンツを個別に追跡するための、エンドユーザ装置109で稼動する処理の流れ図がある。コンテンツID1802は、コンテンツ準備中にコンテンツ・プロバイダ101によって供給される。一実施形態では、コンテンツID1802は、SCパッカー・ツール152を用いるコンテンツ作成処理中にコンテンツSC630の一部になる。もう1つの実施形態では、コンテンツID1802は、メタデータSC620（販売促進データを含む）の一部である。コンテンツID1802は、処理されるコンテンツに固有の識別子である。
【0378】トランザクションID535は、前に上で説明したように、トランザクション・プロセッサ・モジュール175によって作成されるトランザクションSC640内で、コンテンツID1802と共にトランザクション・データ642の一部である。トランザクションID535は、エンドユーザ装置109からの購入トランザクション全体のそれぞれに固有の識別子である。さらに、項目番号1806は、トランザクションの一部を形成する部分またはメンバまたはタイトルのそれぞれについて電子ディジタル・コンテンツ商店103が生成する一意の識別子である。公式の項目番号1806によって、トランザクションID535の下で購入された各項目が追跡される。
【0379】この時のエンドユーザ装置109上の動作に着目すると、エンドユーザ装置109によって受信される。さらに、やはりトランザクションID535内に含まれるコンテンツID1802を含むオファーSCも、受信される。購入ID1812が、エンドユーザ装置109上で作成される。一実施形態では、購入IDは、3つの数、具体的にはコンテンツID1802とトランザクションID535と項目番号1806の連結動作1810である。3つのすべての数字のハッシュ化または、一意の購入ID1812をもたらす他の数学的組合せなど、連結動作1810を除く他の種類の組合せを使用して、購入ID1812を生成することができることを理解されたい。3つの数を組み合わせる処理は、購入ID計算への許可されないアクセスを防ぐために、プレイヤ・アプリケーション内で前に上で説明した耐タンパ・コード技術を使用することにおいて行うことができる。
【0380】一意の購入ID1812が作成され、コンテンツ113の各部分に関連付けられた後に、エンドユーザ装置109のプレイヤ・アプリケーション195は、曲などの同一のコンテンツ113の複数のコピーがエンドユーザ装置109に格納されている場合であっても、コンテンツ113の各部分の商店使用条件519を追跡することができる。
【0381】まとめとして、本発明の構成に関して以下の事項を開示する。
【0382】（1）ディジタル・コンテンツ・プレイヤ上でディジタル・コンテンツをユニークに識別する方法であって、コンテンツ・プロバイダから受信した前記ディジタル・コンテンツをユニークに識別する第1識別子を受信するステップと、前記ディジタル・コンテンツをそれによって受信したトランザクションをユニークに識別する第2識別子を受信するステップと、前記ディジタル・コンテンツをそれによって受信したトランザクション内の項目をユニークに識別する第3識別子を受信するステップと、前記第1識別子、前記第2識別子、および前記第3識別子の数学的組合せに基づいて、第4ユニーク識別子を作るステップとを含む、ディジタル・コンテンツをユニークに識別する方法。
（2）前記作るステップが、前記第1識別子、前記第2識別子、および前記第3識別子の連結に基づいて第4ユニーク識別子を作ることを含む、上記（1）に記載のディジタル・コンテンツをユニークに識別する方法。
（3）前記第2識別子を受信するステップが、前記ディジタル・コンテンツを売る商店からユニークな識別子を受信することを含む、上記（1）に記載のディジタル・コンテンツをユニークに識別する方法。
（4）前記第3識別子を受信するステップが、前記ディジタル・コンテンツを売る商店から、前記ディジタル・コンテンツがそれによって受信されたトランザクションをユニークに識別するユニークな識別子を受信することを含む、上記（3）に記載のディジタル・コンテンツをユニークに識別する方法。
（5）使用条件を含む前記ディジタル・コンテンツに前記第4ユニーク識別子を関連付けるステップと、前記ディジタル・コンテンツを再生する前に、前記第4ユニーク識別子をインデクシングすることによって前記使用条件を再検討するステップとをさらに含む、上記（1）に記載のディジタル・コンテンツをユニークに識別する方法。
（6）第4ユニーク識別子を作る前記ステップが、第4ユニーク識別子への許可されないアクセスを防ぐために、耐タンパ環境で前記第4ユニーク識別子を作ることを含む、上記（1）に記載のディジタル・コンテンツをユニークに識別する方法。
（7）ユーザ装置上でディジタル・コンテンツの使用を追跡するシステムであって、コンピュータ可読媒体上でディジタル・コンテンツをユーザに配布する複数のコンテンツ・サイトであって、前記ディジタル・コンテンツが、それに関連付けられたユニークなコンテンツ識別子を含む、複数のコンテンツ・サイトと、ディジタル・コンテンツ・データを再生するライセンスをユーザに与える複数の電子商店であって、各電子商店が、ネットワークに結合され、前記ライセンスが、トランザクションをユニークに識別するユニークなトランザクション識別子を含み、前記ライセンスが、前記トランザクション内の少なくとも1つの項目をユニークに識別するユニークな項目識別子を含む、複数の電子商店と、コンテンツ・データを再生する複数のコンテンツ・プレイヤであって、各ディジタル・コンテンツ・プレイヤが、前記ユーザのうちの1つによってライセンスを交付された前記ディジタル・コンテンツ・データを前記ネットワークから受信し、前記コンテンツ・プレイヤが、前記コンテンツ識別子、前記トランザクション識別子、および前記項目識別子の数学的組合せに基づいて購入識別子を作る、複数のコンテンツ・プレイヤとを含む、ユーザ装置上でディジタル・コンテンツの使用を追跡するシステム。
（8）前記数学的組合せが、連結である、上記（7）に記載のユーザ装置上でディジタル・コンテンツの使用を追跡するシステム。
（9）前記コンテンツ・プレイヤが、耐タンパ環境を含み、前記購入識別子が、それへの許可されないアクセスを防ぐために、前記耐タンパ環境内で作られる、上記（7）に記載のユーザ装置上でディジタル・コンテンツの使用を追跡するシステム。
（10）ディジタル・コンテンツをユニークに識別するディジタル・コンテンツ・プレイヤであって、コンテンツ・プロバイダから受信した前記ディジタル・コンテンツをユニークに識別する第1識別子を受信する手段と、前記ディジタル・コンテンツがそれによって受信されたトランザクションをユニークに識別する第2識別子を受信する手段と、前記ディジタル・コンテンツがそれによって受信されたトランザクション内の項目をユニークに識別する第3識別子を受信する手段と、前記第1識別子、前記第2識別子、および前記第3識別子の数学的組合せに基づいて第4ユニーク識別子を作る手段とを含む、ディジタル・コンテンツをユニークに識別するディジタル・コンテンツ・プレイヤ。

(11)前記作る手段が、前記第1識別子、前記第2識別子、および前記第3識別子の連結に基づいて第4ユニーク識別子を作ることを含む、上記(10)に記載のディジタル・コンテンツをユニークに識別するディジタル・コンテンツ・プレイヤ。
(12)前記第2識別子を受信する手段が、前記ディジタル・コンテンツを売る商店からユニークな識別子を受信することを含む、上記(10)に記載のディジタル・コンテンツをユニークに識別するディジタル・コンテンツ・プレイヤ。
(13)前記第3識別子を受信する手段が、前記ディジタル・コンテンツを売る商店から、前記ディジタル・コンテンツがそれによって受信されたトランザクションをユニークに識別するユニークな識別子を受信することを含む、上記(10)に記載のディジタル・コンテンツをユニークに識別するディジタル・コンテンツ・プレイヤ。
(14)使用条件を含む前記ディジタル・コンテンツに前記第4ユニーク識別子を関連付ける手段と、前記ディジタル・コンテンツを再生する前に、前記第4ユニーク識別子をインデクシングすることによって前記使用条件を再検討する手段とをさらに含む、上記(10)に記載のディジタル・コンテンツをユニークに識別するディジタル・コンテンツ・プレイヤ。
(15)ディジタル・コンテンツ・プレイヤ上でディジタル・コンテンツをユニークに識別するプログラム命令を含むコンピュータ可読媒体であって、コンテンツ・プロバイダから受信した前記ディジタル・コンテンツをユニークに識別する第1識別子を受信するプログラム命令と、前記ディジタル・コンテンツをそれによって受信したトランザクションをユニークに識別する第2識別子を受信するプログラム命令と、前記ディジタル・コンテンツをそれによって受信したトランザクション内の項目をユニークに識別する第3識別子を受信するプログラム命令と、前記第1識別子、前記第2識別子、および前記第3識別子の数学的組合せに基づいて、第4ユニーク識別子を作るプログラム命令とを含む、コンピュータ可読媒体。
(16)前記作るプログラム命令が、前記第1識別子、前記第2識別子、および前記第3識別子の連結に基づいて第4ユニーク識別子を作ることを含む、上記(15)に記載のコンピュータ可読媒体。
(17)前記第2識別子を受信するプログラム命令が、前記ディジタル・コンテンツを売る商店からユニークな識別子を受信することを含む、上記(15)に記載のコンピュータ可読媒体。
(18)前記第3識別子を受信するプログラム命令が、前記ディジタル・コンテンツを売る商店から、前記ディジタル・コンテンツがそれによって受信されたトランザクションをユニークに識別するユニークな識別子を受信することを含む、上記(17)に記載のコンピュータ可読媒体。
(19)使用条件を含む前記ディジタル・コンテンツに前記第4ユニーク識別子を関連付けるプログラム命令と、前記ディジタル・コンテンツを再生する前に、前記第4ユニーク識別子をインデクシングすることによって前記使用条件を再検討するプログラム命令とをさらに含む、上記(15)に記載のコンピュータ可読媒体。
(20)第4ユニーク識別子を作る前記プログラム命令が、第4ユニーク識別子への許可されないアクセスを防ぐために、耐タンパ環境で前記第4ユニーク識別子を作ることを含む、上記(15)に記載のコンピュータ可読媒体。

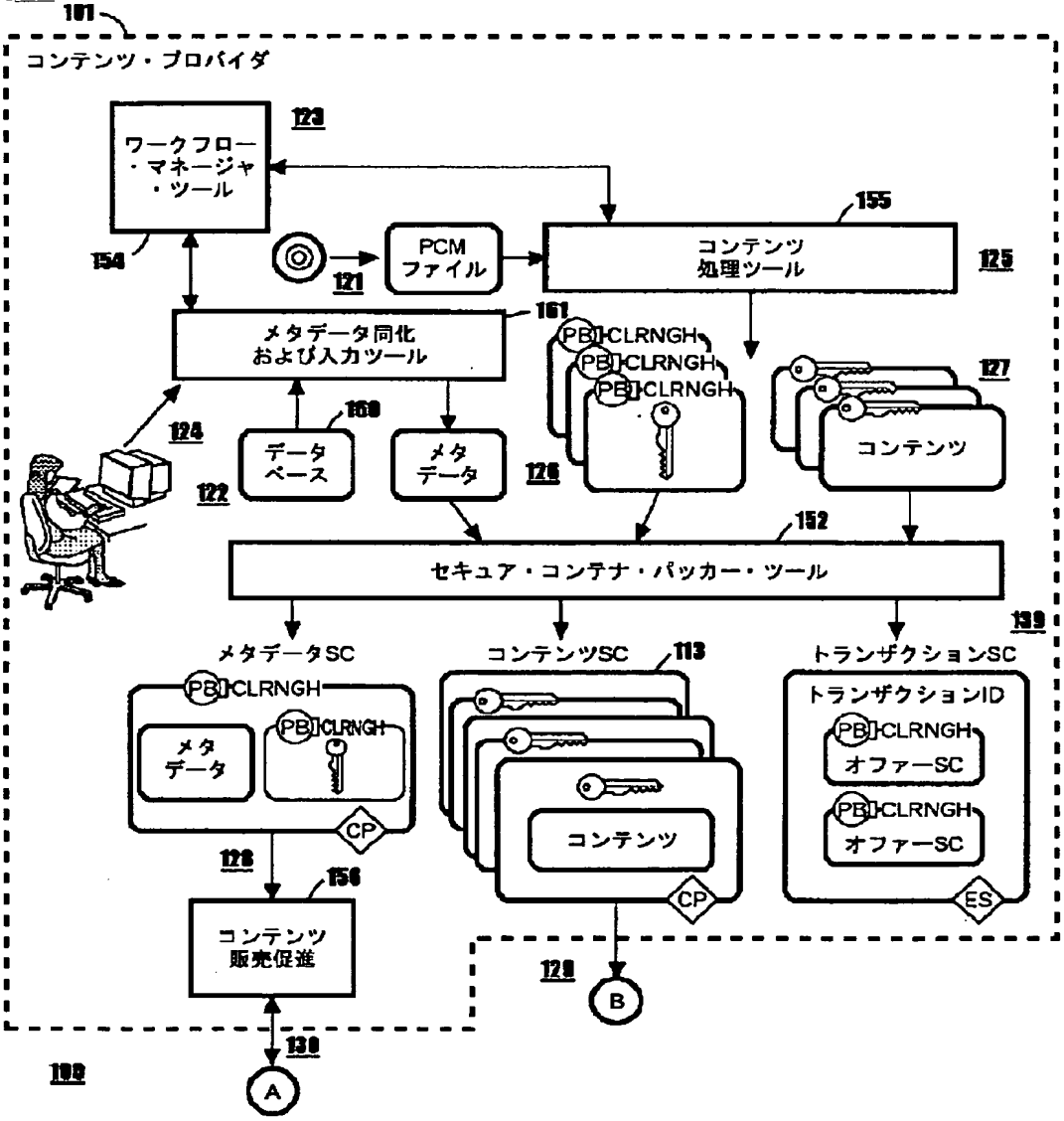
図の説明

【図面の簡単な説明】
【図1】本発明による、セキュア・ディジタル・コンテンツ電子配布システムの概要を示すブロック図の一部である。
【図2】本発明による、セキュア・ディジタル・コンテンツ電子配布システムの概要を示すブロック図の一部である。
【図3】本発明による、セキュア・ディジタル・コンテンツ電子配布システムの概要を示すブロック図の一部である。
【図4】本発明による、セキュア・ディジタル・コンテンツ電子配布システムの概要を示すブロック図の一部である。
【図5】本発明による、例のセキュア・コンテナ(SC)および関連するグラフィカル表現を示すブロック図である。
【図6】本発明による、セキュア・コンテナ(SC)の暗号化処理の概要を示すブロック図である。
【図7】本発明による、セキュア・コンテナ(SC)の暗号解読の概要を示すブロック図である。
【図8】本発明による、図1ないし4のセキュアイ・ディジタル・コンテンツ配布システムの権利管理アーキテクチャの諸層の概要を示すブロック図である。
【図9】図8のライセンス制御層に適用される、コンテンツ配布およびライセンス交付制御の概要を示すブロック図である。
【図10】本発明による、図1ないし4のワーク・フロー・マネージャ・ツールの例のユーザ・インターフェースを示す図である。
【図11】本発明による、図10のユーザ・インターフェースに対応するワーク・フロー・マネージャの主要なツール、コンポーネント、および処理のブロック図である。
【図12】本発明による、図1ないし4の電子ディジタル・コンテンツ商店の主要なツール、コンポーネント、および処理を示すブロック図である。
【図13】本発明による、図1ないし4のエンドユーザ装置の主要なコンポーネントおよび処理を示すブロック図である。
【図14】本発明による、図11のコンテンツ前処理および圧縮ツールの符号化率係数を計算する方法の流れ図である。
【図15】本発明による、図11の自動メタデータ獲得ツールの、追加情報を自動的に取り出す方法の流れ図である。
【図16】本発明による、図11の前処理および圧縮ツールの、前処理パラメータおよび圧縮パラメータを自動的に設定する方法の流れ図である。
【図17】本発明による、図18および図19に記載のようにローカル・ライブラリにコンテンツをダウンロードする、プレイヤ・アプリケーションのユーザ・インターフェース画面の例を示す図である。
【図18】本発明による、図12のエンドユーザ装置で稼動するプレイヤ・アプリケーションの主要なコンポーネントおよび処理を示すブロック図である。
【図19】本発明による、図12のエンドユーザ装置で稼動するプレイヤ・アプリケーションの主要なコンポーネントおよび処理を示すブロック図である。
【図20】本発明による、図18および図19のプレイヤ・アプリケーションの例のユーザ・インターフェース画面を示す図である。
【図21】本発明による、図11の自動メタデータ獲得ツールの、追加情報を自動的に取り出すための代替実施形態の流れ図である。
【図22】本発明による、コンテンツを個別に追跡するための、エンドユーザ装置109で稼動する処理の流れ図である。
【符号の説明】
100 セキュア・ディジタル・コンテンツ電子配布システム
101 コンテンツ・プロバイダ
103 電子ディジタル・コンテンツ商店
105 クリアリングハウス
109 エンドユーザ装置
501 ライセンス制御層
502 コンテンツ前処理
503 コンテンツ識別層
505 コンテンツ使用制御層

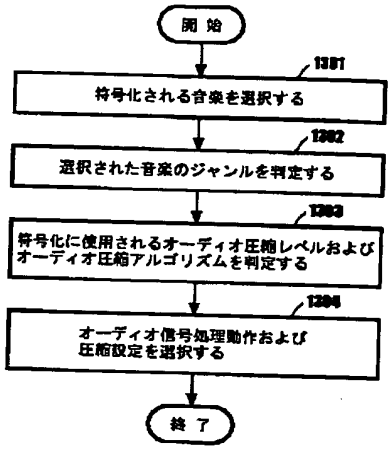
507 コンテンツ・フォーマッティング層
801 処置／情報待機中製品処理
802 新規コンテンツ要求処理
803 自動メタデータ獲得処理
804 手動メタデータ入力処理
805 使用条件処理
806 監視公開処理
807 メタデータSC作成処理
808 ウォーターマーキング処理
809 前処理および圧縮処理
810 コンテンツ品質管理処理
811 暗号化処理
812 コンテンツSC作成処理
813 最終品質保証処理
814 コンテンツ分散処理

図面

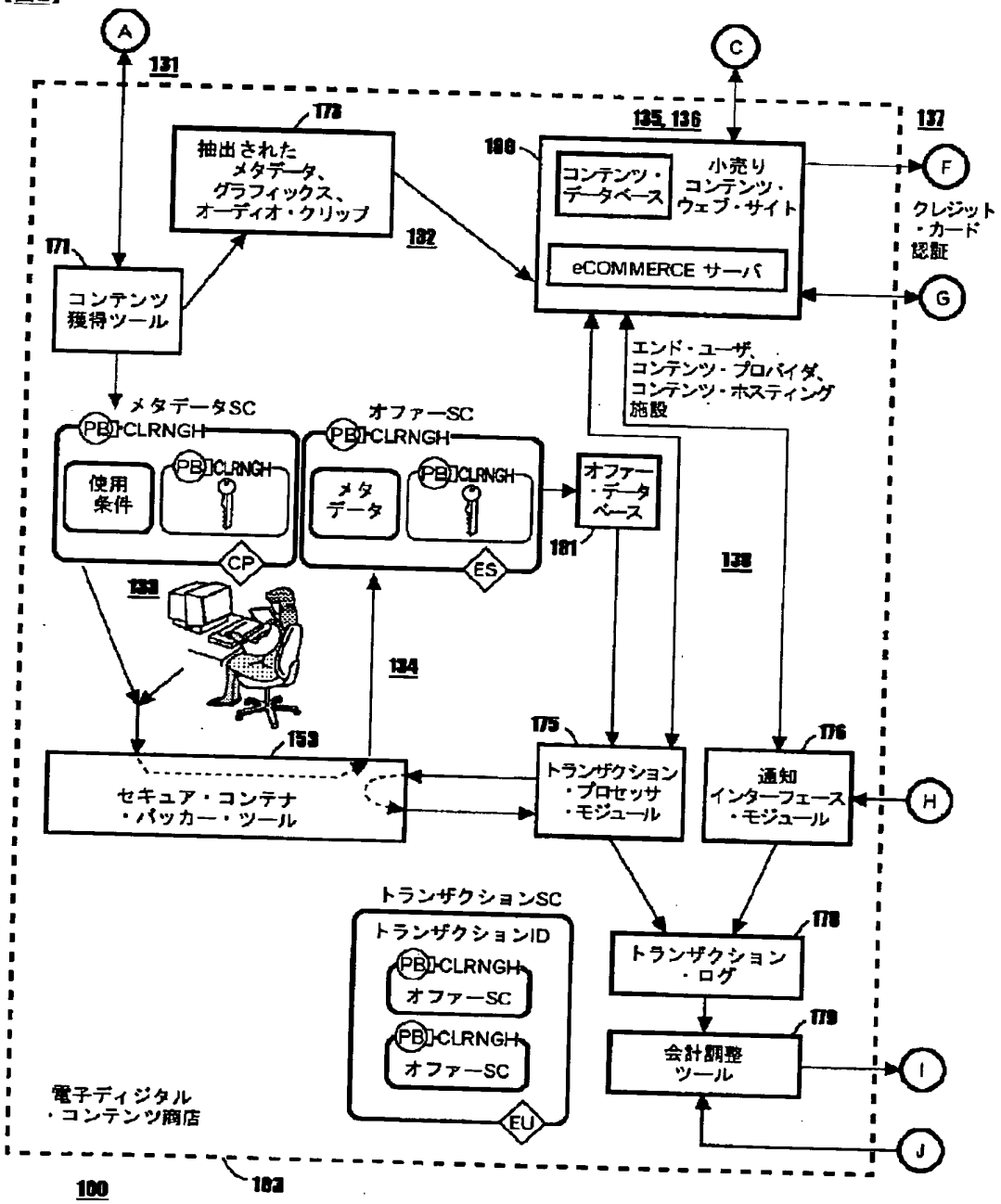
【図1】



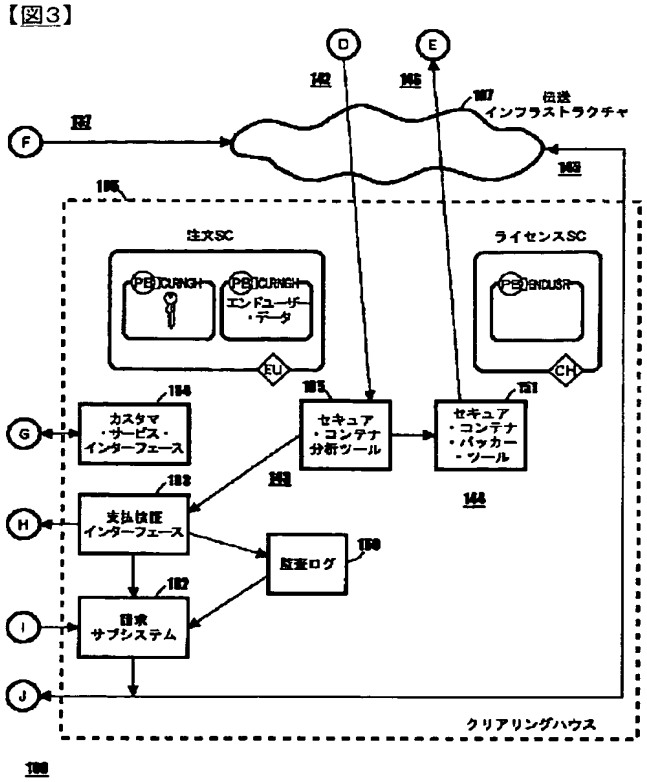
【図16】


開始
1301
符号化される音楽を選択する
1302
選択された音楽のジャンルを判定する
1303
符号化に使用されるオーディオ圧縮レベルおよびオーディオ圧縮アルゴリズムを判定する
1304
オーディオ信号処理動作および圧縮設定を選択する
終了

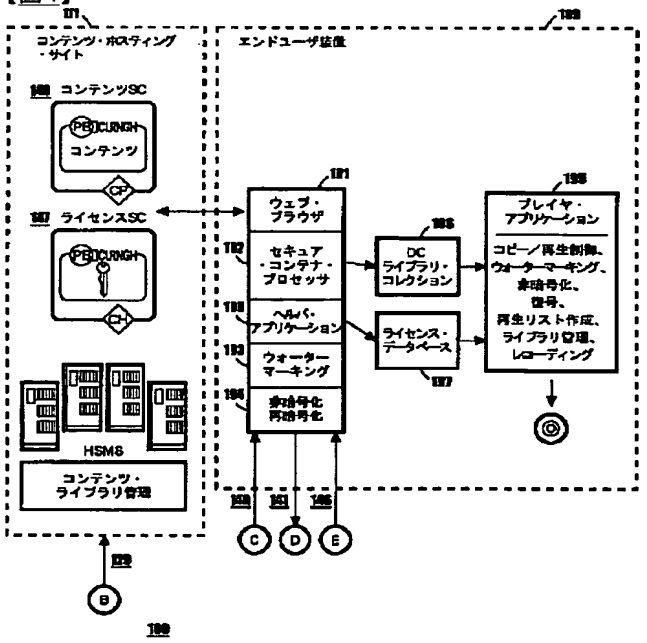
【図2】


A
131
C
178
抽出された
メタデータ、
グラフィックス、
オーディオ・クリップ
135, 136
137
180
コンテンツ・
データベース
小売り
コンテンツ・
ウェブ・サイト
F
クレジット
・カード
認証
171
132
eCOMMERCE サーバ
G
コンテンツ
獲得ツール
エンド・ユーザ、
コンテンツ・プロバイダ、
コンテンツ・ホスティング
施設
メタデータSC
PBI
CLRNGH
使用
条件
CP
オファーSC
メタ
データ
ES
オファー
・データ
ベース
181
138
150
134
153
175
176
セキュア・コンテナ
・パッカー・ツール
トランザクション
・プロセッサ
・モジュール
通知
インターフェース
・モジュール
H
トランザクションSC
トランザクションID
オファーSC
178
トランザクション
・ログ
179
会計調整
ツール
I
J
EU
電子ディジタル
・コンテンツ商店
100
182

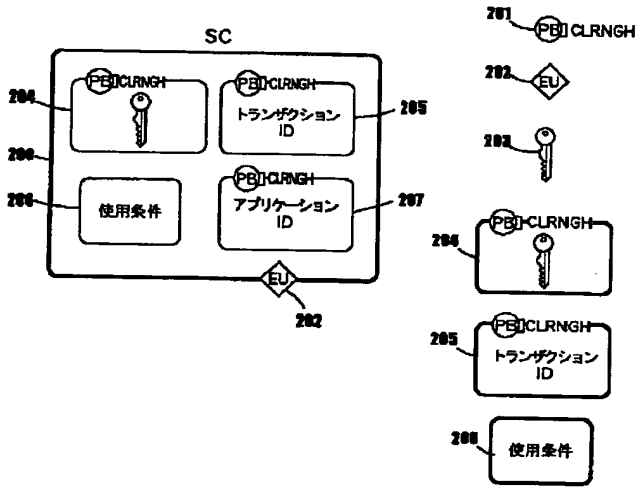
【図3】


D
E
142
145
147
伝送
インフラストラクチャ
F
152
153
155
注文SC
ライセンスSC
PEI CURRIGH
エンドユーザ・データ
PEI ENDUSR
EU
CH
154
カスタマ・サービス・インターフェース
G
セキュア・コンテナ分析ツール
151
セキュア・コンテナ・パッカー・ツール
144
152
支払仲介インターフェース
H
158
監査ログ
157
請求サブシステム
I
J
クリアリングハウス
150

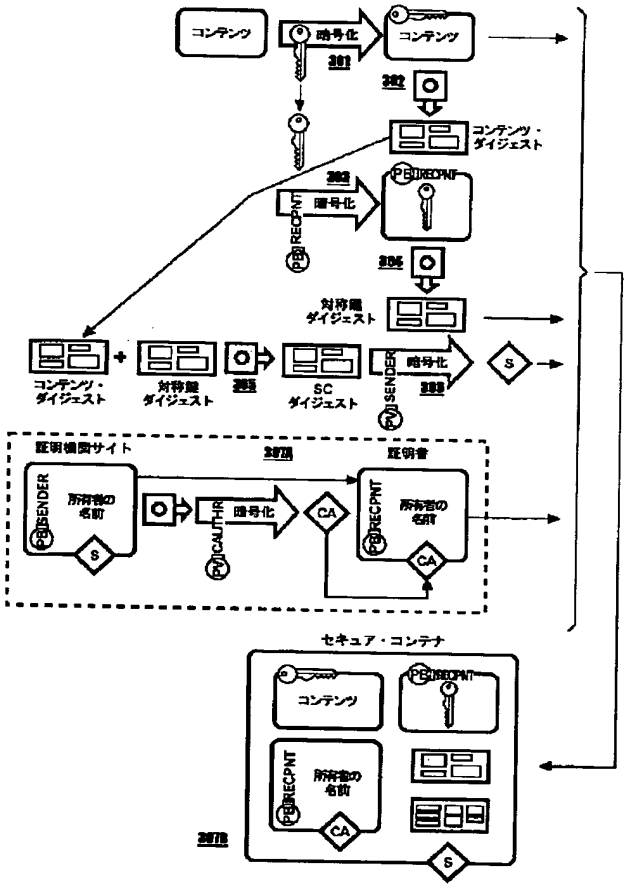
【図4】


171
コンテンツ・ホスティング・サイト
169
エンドユーザ装置
160
コンテンツSC
PEI CURRIGH
コンテンツ
CP
167
ライセンスSC
CH
HSMS
コンテンツ・ライブラリ管理
172
B
170
171
ウェブ・ブラウザ
172
セキュア・コンテナ・プロセッサ
173
ヘルパ・アプリケーション
174
ウォーターマーキング
175
暗号化再暗号化
176
DC ライブラリ・コレクション
177
ライセンス・データベース
178
プレイヤ・アプリケーション
コピー／再生制御、ウォーターマーキング、非暗号化、復号、再生リスト作成、ライブラリ管理、レコーディング
C
D
E

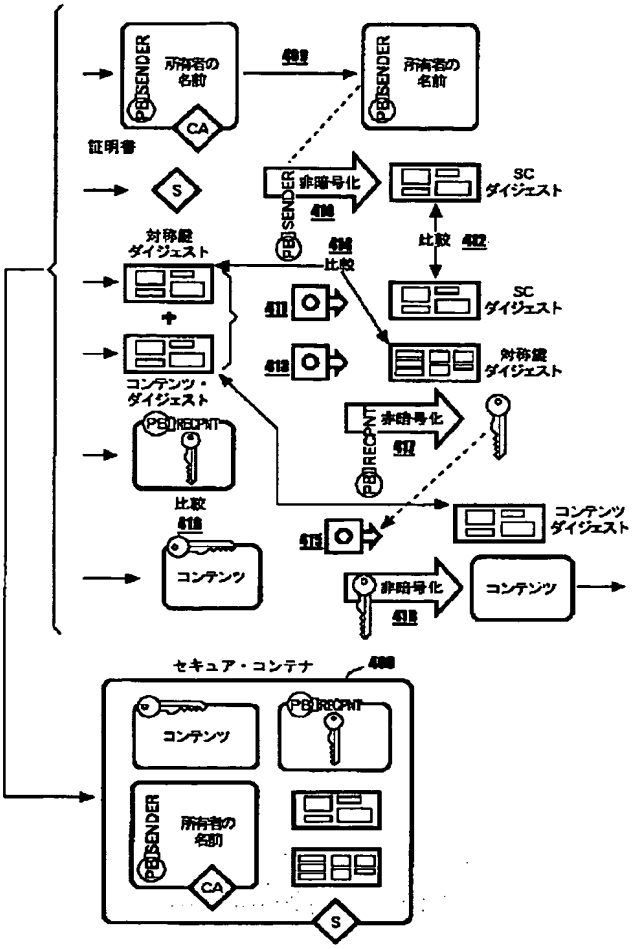
【図5】


SC
PB CLRNGH
トランザクション ID
使用条件
アプリケーション ID
EU
201
202
203
204
205
206
207
208

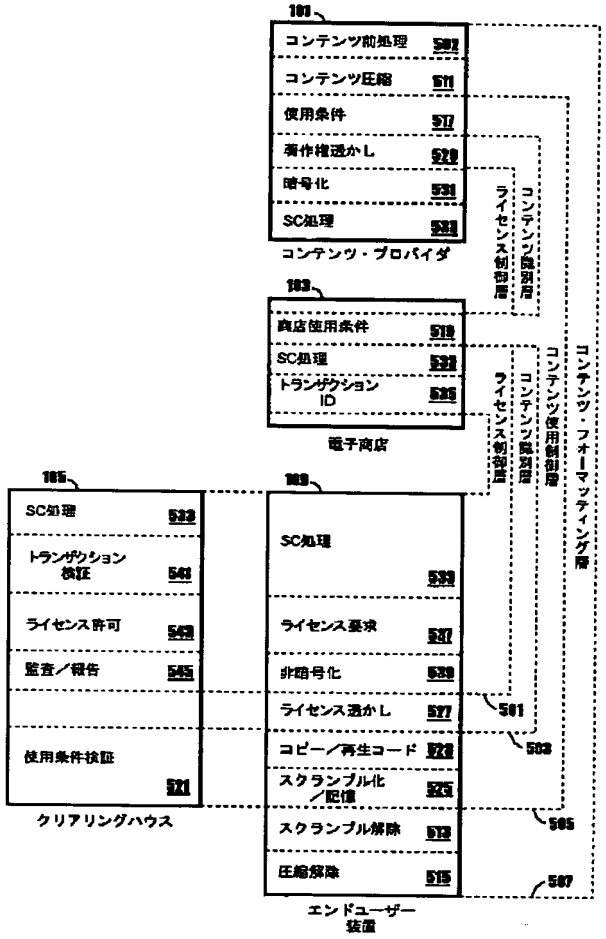
【図6】


コンテンツ
暗号化
コンテンツ
コンテンツ・ダイジェスト
PB RECPNT
対称鍵 ダイジェスト
SC ダイジェスト
PB SENDER
S
証明機関サイト
証明書
所有者の名前
PB CAUTHR
CA
セキュア・コンテナ

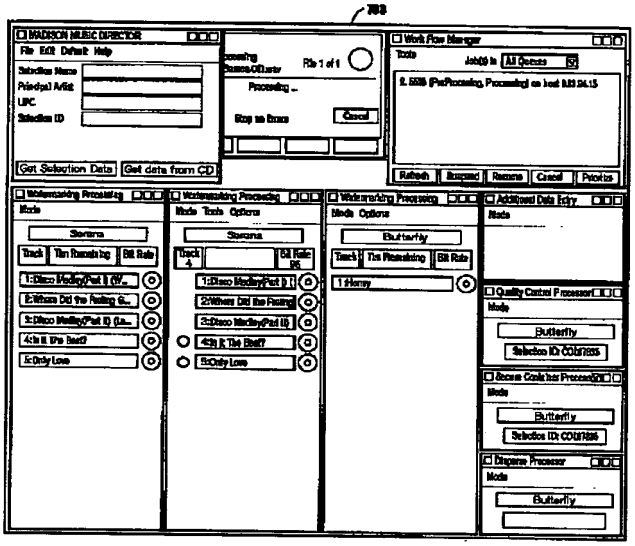
【図7】


所有者の名前
PBSENDER
CA
証明書
S
非暗号化
SC ダイジェスト
比較
対称鍵 ダイジェスト
コンテンツ・ダイジェスト
PBRECPNT
コンテンツ
セキュア・コンテナ

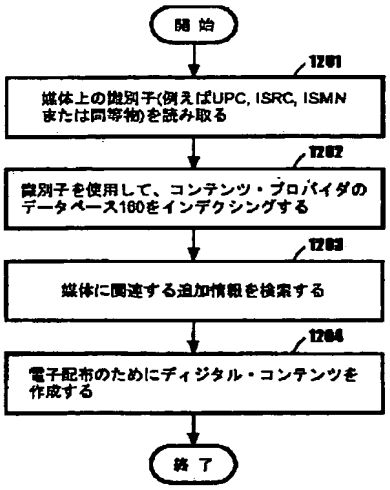
【図8】


コンテンツ前処理
コンテンツ圧縮
使用条件
著作権透かし
暗号化
SC処理
コンテンツ・プロバイダ
ライセンス制御層
コンテンツ識別層
商店使用条件
SC処理
トランザクション ID
電子商店
コンテンツ使用制御層
コンテンツ・フォーマッティング層
SC処理
トランザクション検証
ライセンス許可
監査／報告
使用条件検証
クリアリングハウス
SC処理
ライセンス基準
非暗号化
ライセンス透かし
コピー／再生コード
スクランブル化／配信
スクランブル解除
圧縮解除
エンドユーザー装置

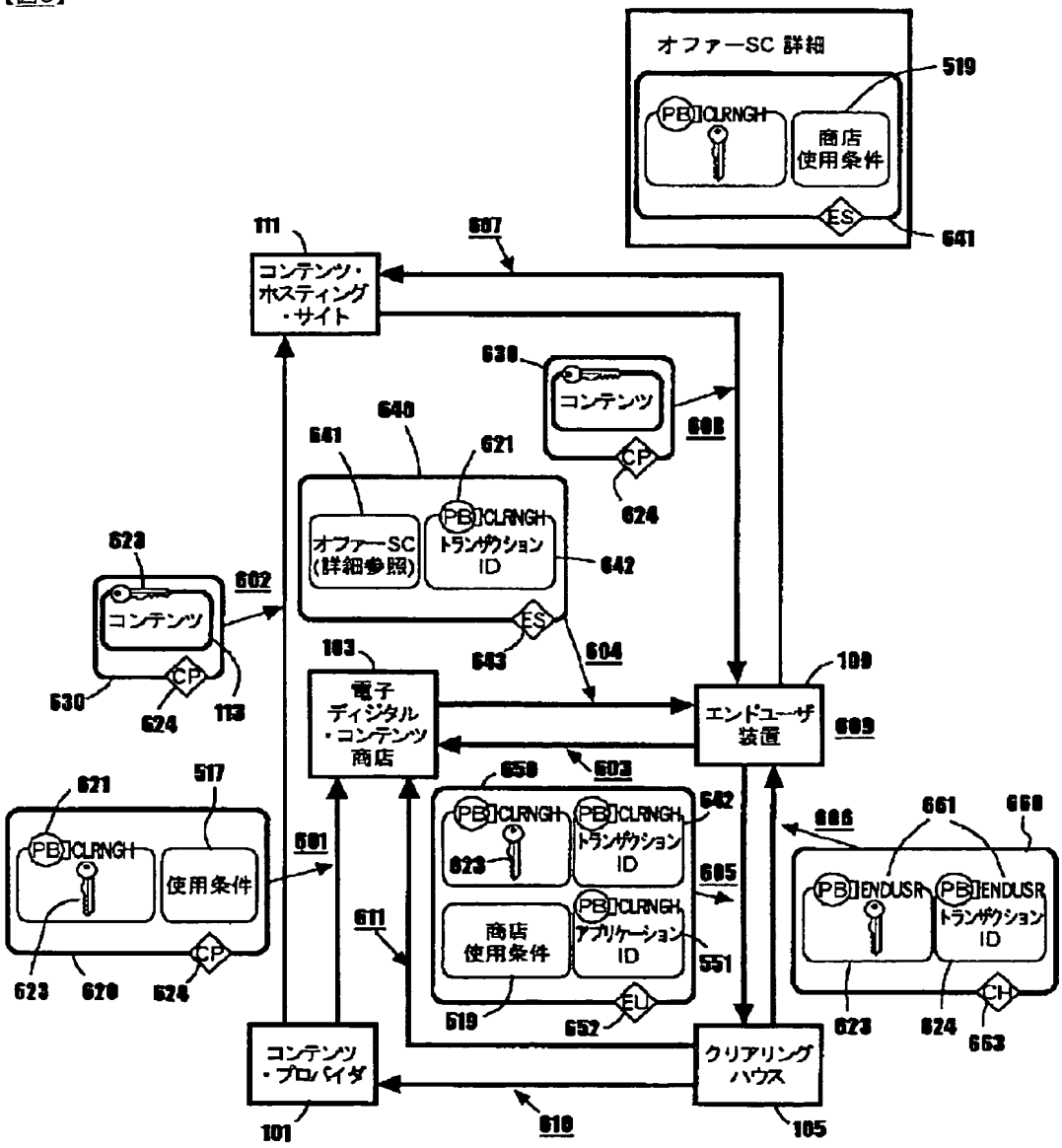
【図10】



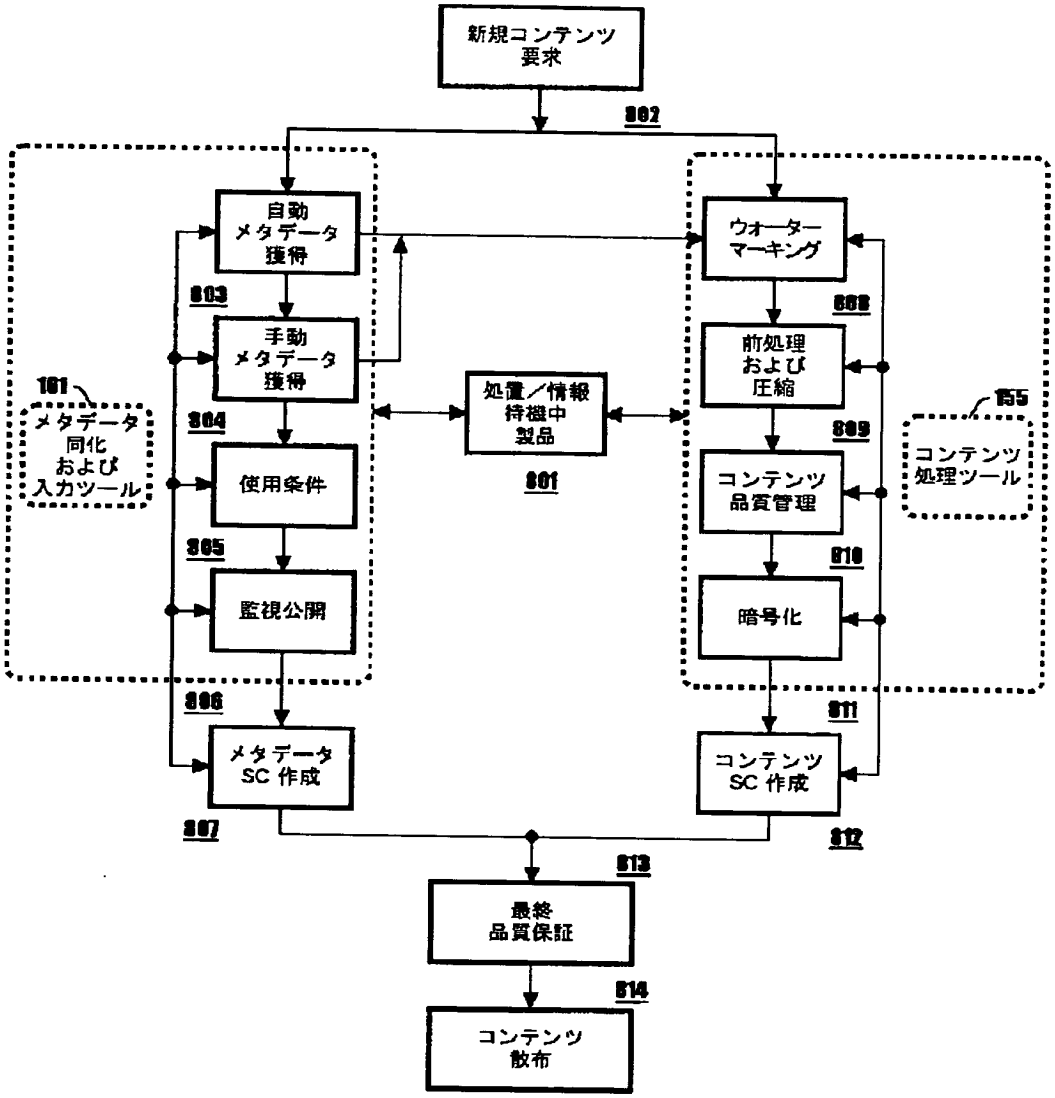
【図15】


開始
1201
媒体上の識別子(例えばUPC, ISRC, ISMNまたは同等物)を読み取る
1202
識別子を使用して、コンテンツ・プロバイダのデータベース160をインデクシングする
1203
媒体に関連する追加情報を検索する
1204
電子配布のためにディジタル・コンテンツを作成する
終了

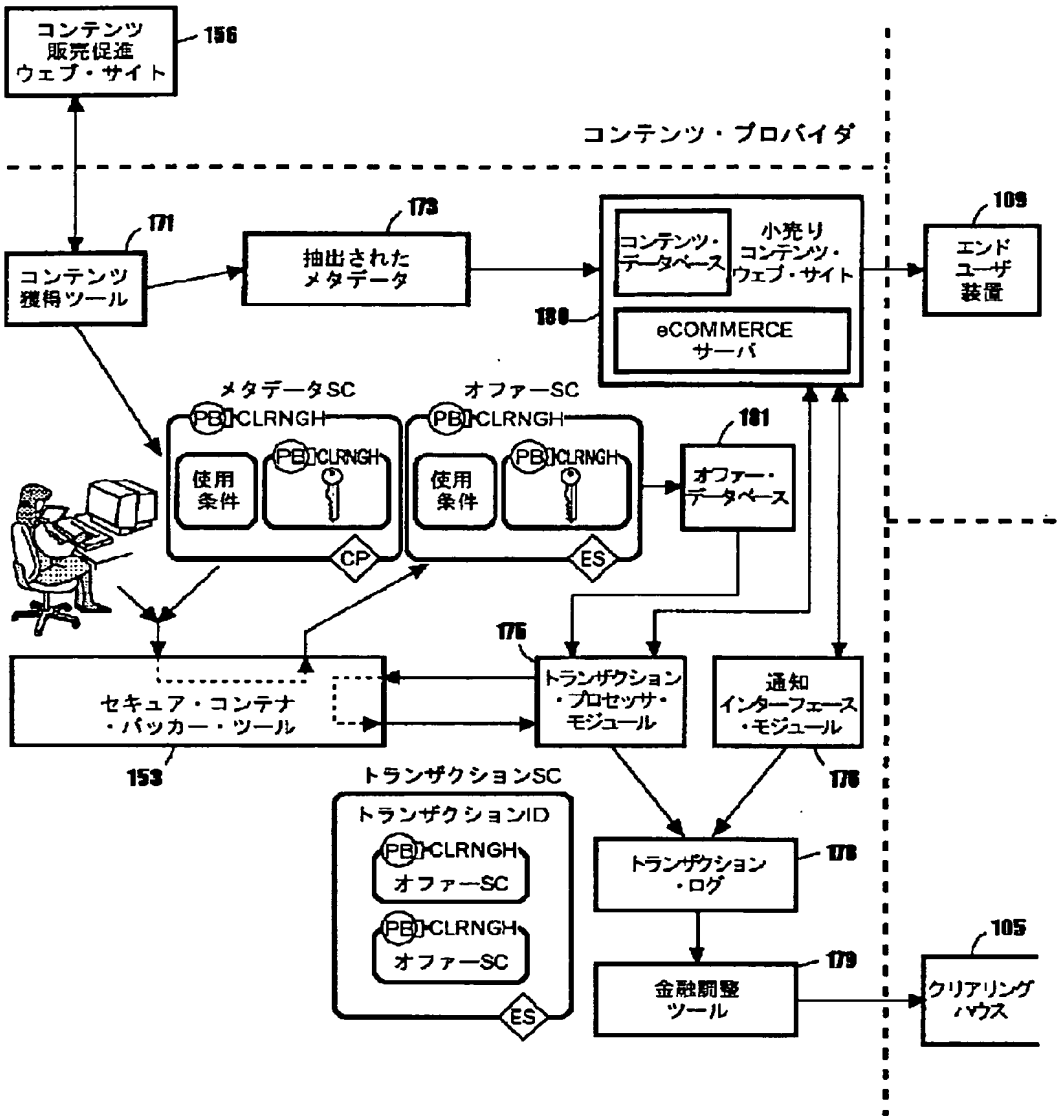
【図9】


オファーSC 詳細
519
PB CLRNGH
商店使用条件
ES
641
111
607
コンテンツ・ホスティング・サイト
638
コンテンツ
608
CP
624
640
641
621
PB CLRNGH
オファーSC(詳細参照)
トランザクションID
642
ES
643
604
623
602
コンテンツ
CP
630
624
113
103
電子ディジタル・コンテンツ商店
109
エンドユーザ装置
609
603
658
642
PB CLRNGH
PB CLRNGH
623
トランザクションID
605
PB CLRNGH
アプリケーションID
551
商店使用条件
519
EU
652
621
517
PB CLRNGH
使用条件
601
CP
623
620
624
611
606
661
658
PB ENDUSR
PB ENDUSR
トランザクションID
CH
623
624
653
コンテンツ・プロバイダ
101
618
クリアリングハウス
105

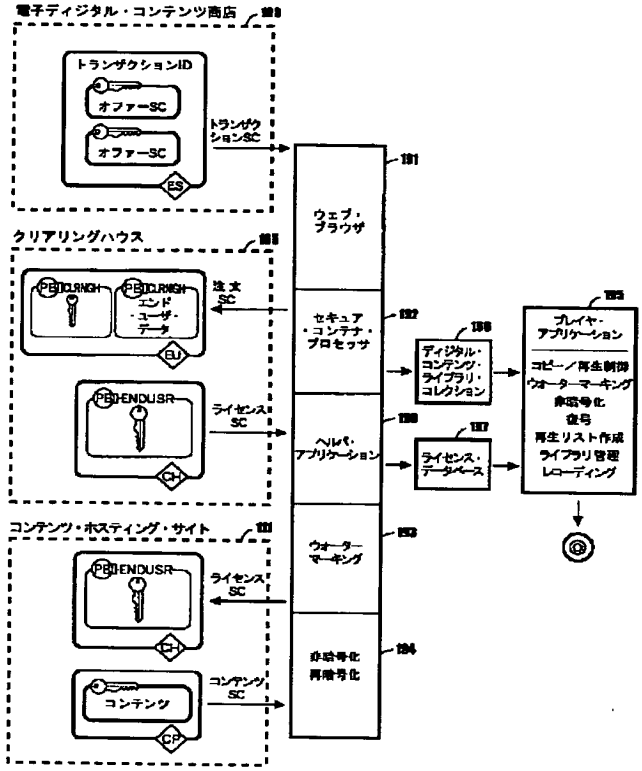
【図11】


新規コンテンツ要求
802
自動メタデータ獲得
803
手動メタデータ獲得
804
使用条件
805
監視公開
806
メタデータSC作成
807
ウォーターマーキング
808
前処理および圧縮
809
コンテンツ品質管理
810
暗号化
811
コンテンツSC作成
812
813
最終品質保証
814
コンテンツ散布
801
処置／情報持機中製品
101
メタデータ同化および入力ツール
155
コンテンツ処理ツール

【図12】

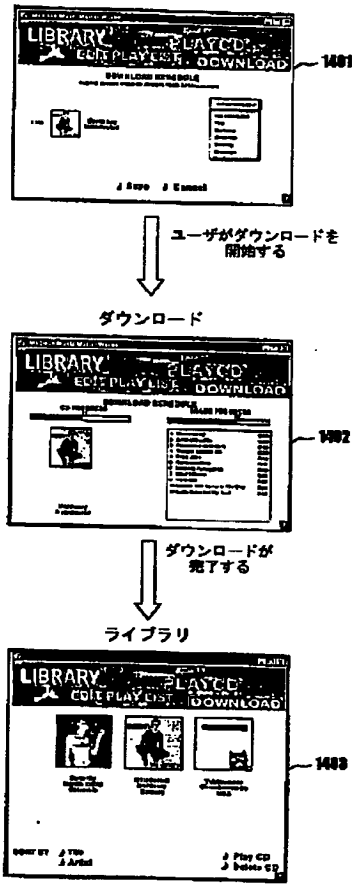

コンテンツ
販売促進
ウェブ・サイト
156
コンテンツ・プロバイダ
171
コンテンツ
獲得ツール
173
抽出された
メタデータ
コンテンツ・
データベース
小売り
コンテンツ・
ウェブ・サイト
109
エンド
ユーザ
装置
180
eCOMMERCE
サーバ
メタデータSC
オファーSC
PBI
CLRNGH
使用
条件
CP
ES
181
オファー・
データベース
175
トランザクション
・プロセッサ・
モジュール
通知
インターフェース
・モジュール
セキュア・コンテナ
・パッカー・ツール
153
176
トランザクションSC
トランザクションID
オファーSC
178
トランザクション
・ログ
179
金融調整
ツール
105
クリアリング
ハウス

【図13】

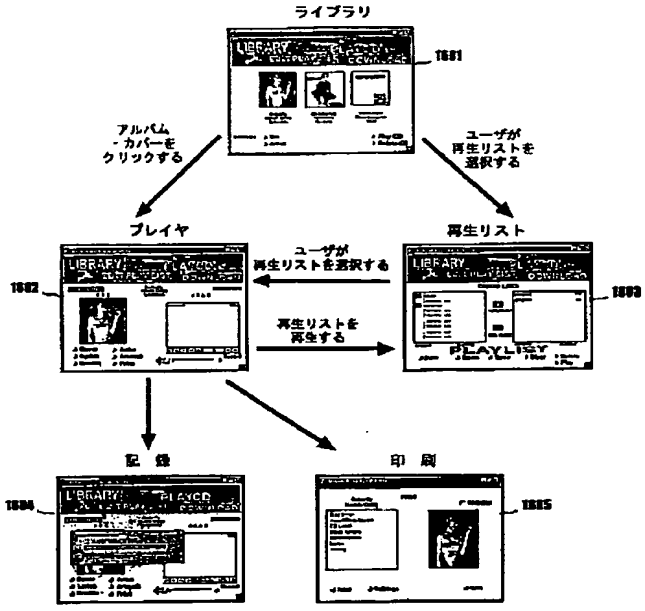


【図17】

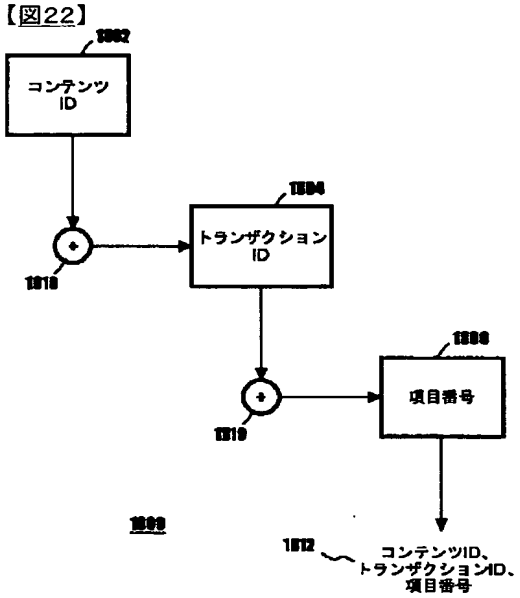
ダウンロードをスケジューリングする



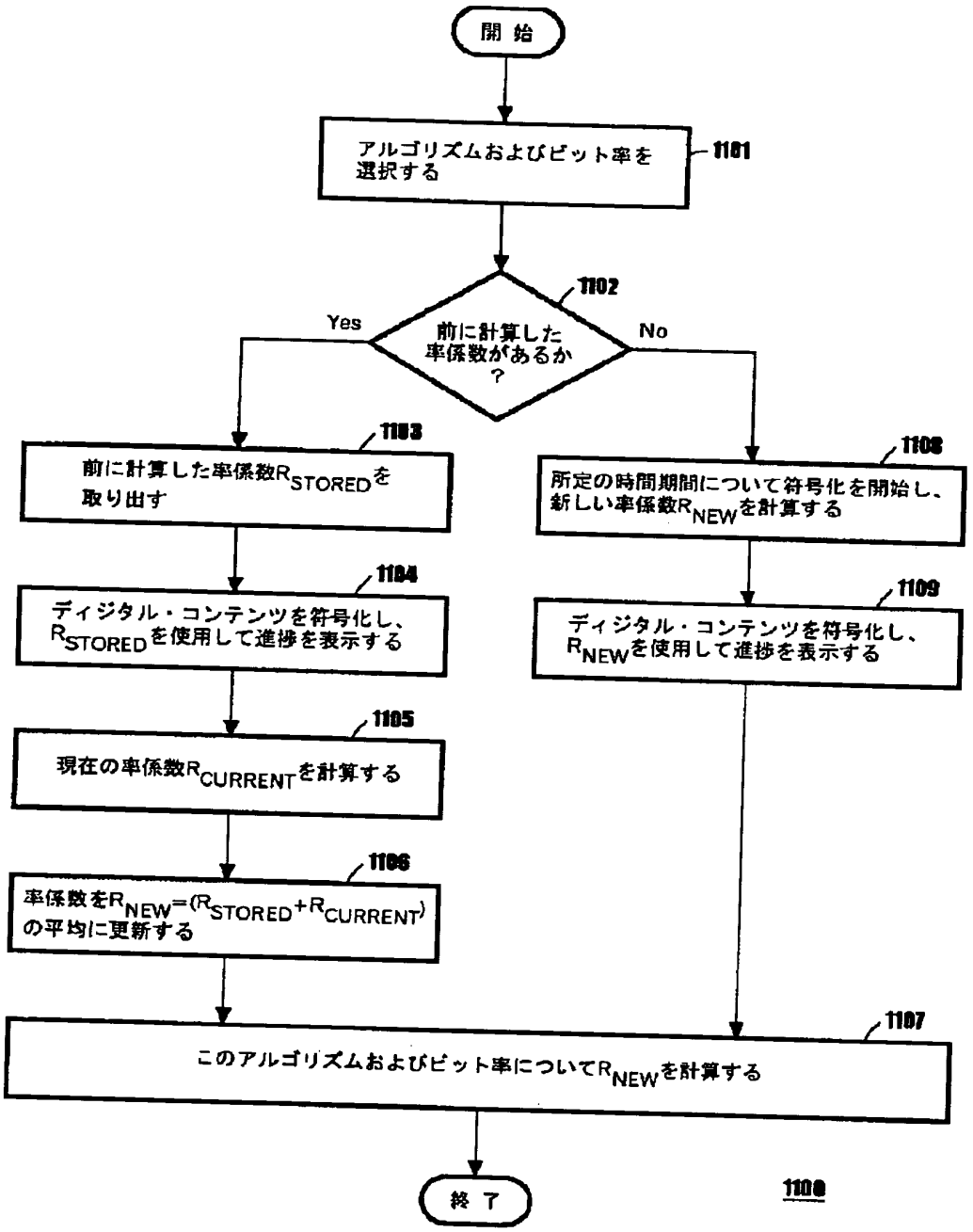
【図20】


ライブラリ
1881
アルバム・カバーをクリックする
ユーザが再生リストを選択する
プレイヤ
再生リスト
ユーザが再生リストを選択する
再生リストを再生する
1882
1883
記録
印刷
1884
1885

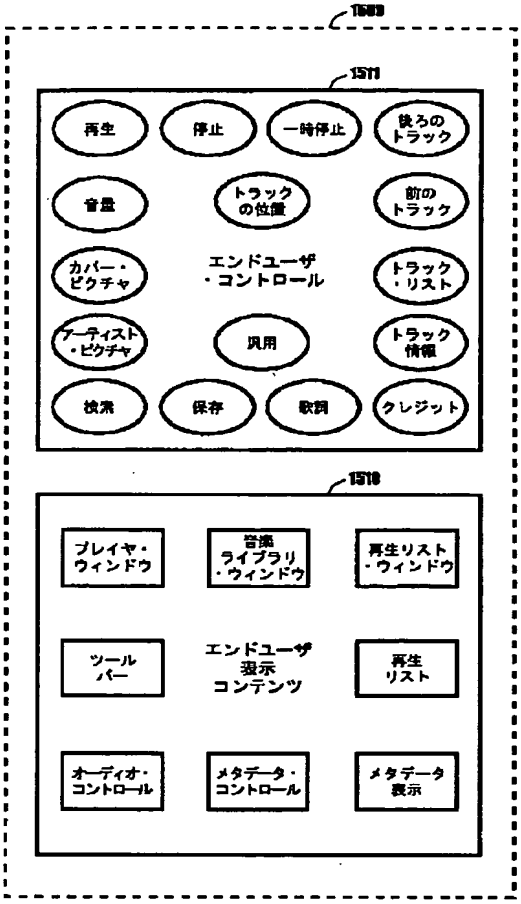
【図22】


1902
コンテンツID
1904
トランザクションID
1910
1908
項目番号
1919
1909
1912
コンテンツID、
トランザクションID、
項目番号

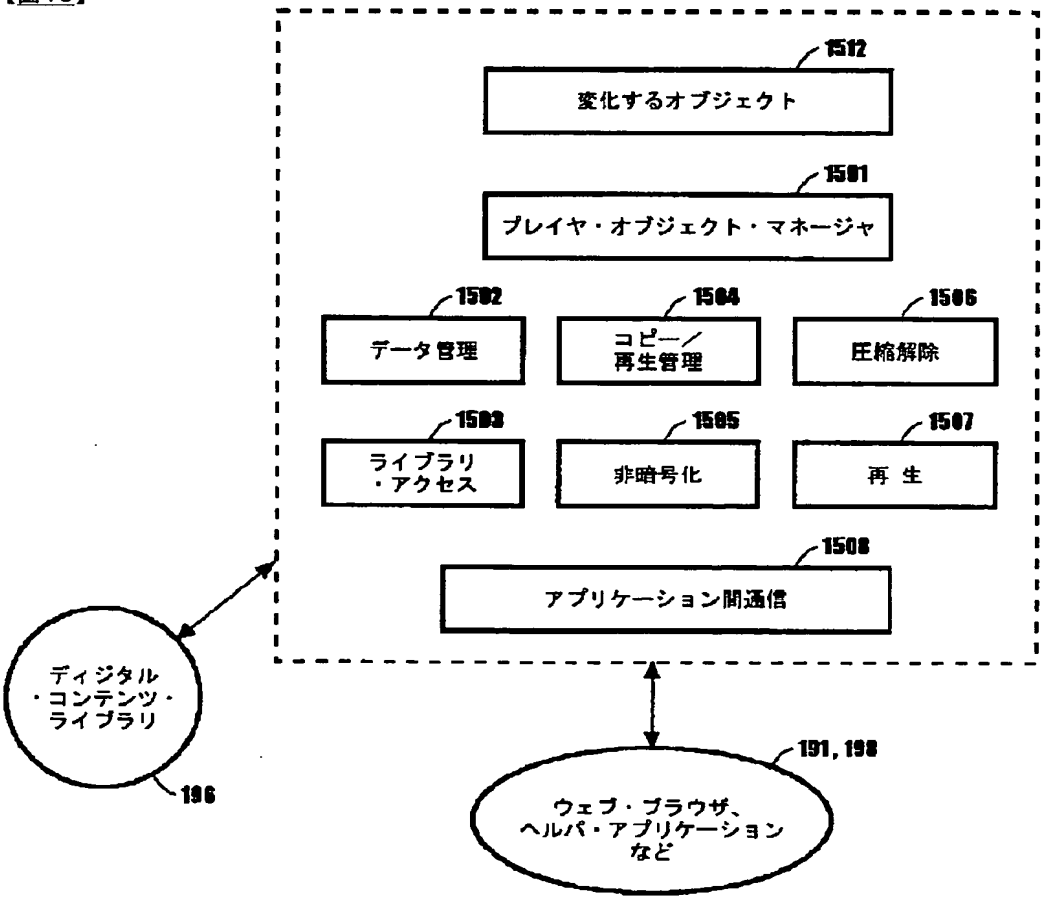
【図14】


開始
アルゴリズムおよびビット率を選択する
1101
1102
前に計算した率係数があるか？
Yes
No
1103
前に計算した率係数R_{STORED}を取り出す
1104
ディジタル・コンテンツを符号化し、R_{STORED}を使用して進捗を表示する
1105
現在の率係数$R_{CURRENT}$を計算する
1106
率係数を$R_{NEW}=(R_{STORED}+R_{CURRENT})$の平均に更新する
1108
所定の時間期間について符号化を開始し、新しい率係数R_{NEW}を計算する
1109
ディジタル・コンテンツを符号化し、R_{NEW}を使用して進捗を表示する
1107
このアルゴリズムおよびビット率についてR_{NEW}を計算する
終了
1100

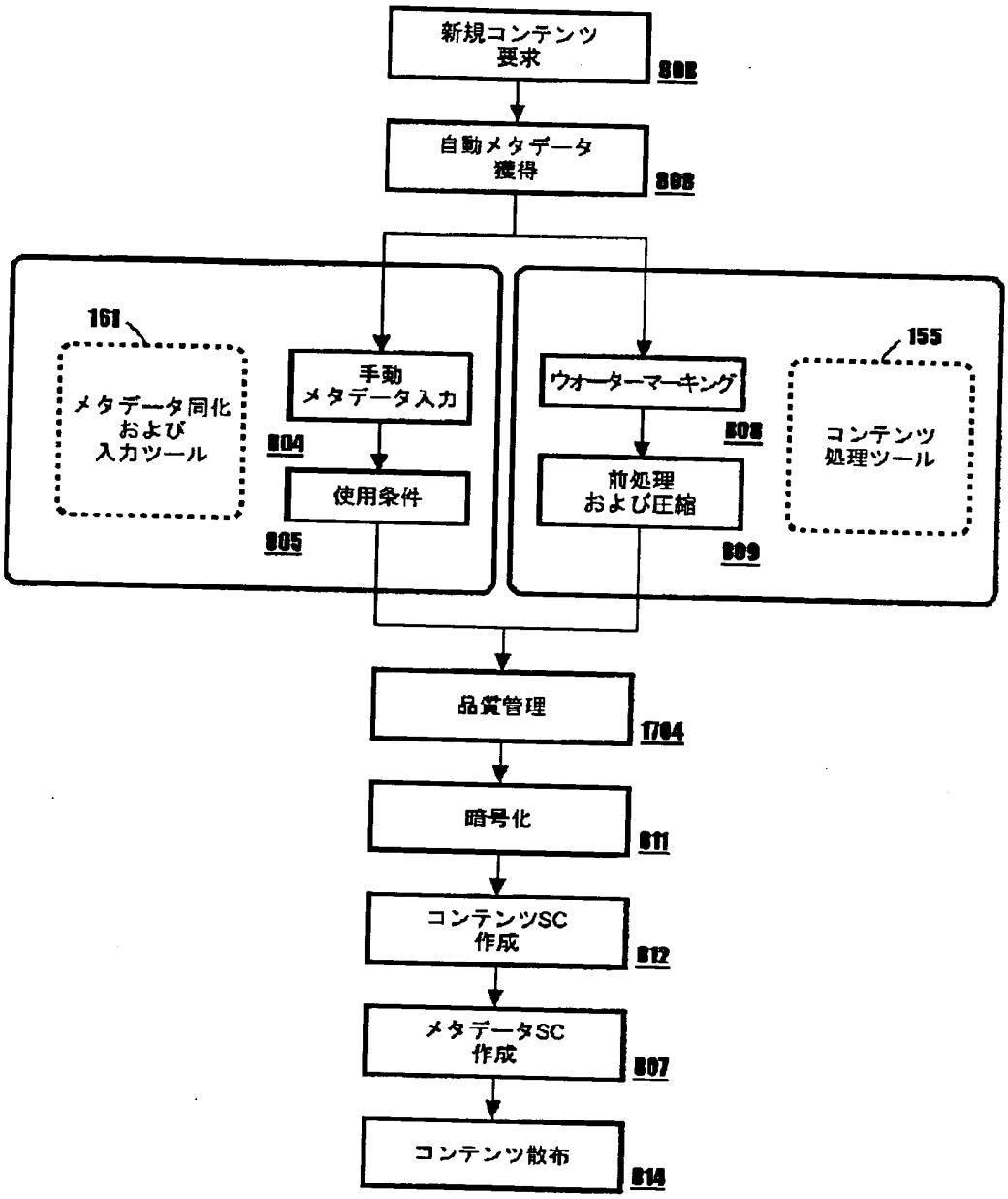
【図18】


1513
1511
再生
停止
一時停止
後ろの
トラック
音量
トラック
の位置
前の
トラック
カバー・
ピクチャ
エンドユーザ
・コントロール
トラック
・リスト
アーティスト
・ピクチャ
汎用
トラック
情報
検索
保存
歌詞
クレジット
1510
プレイヤ・
ウィンドウ
音楽
ライブラリ
・ウィンドウ
再生リスト
・ウィンドウ
ツール
バー
エンドユーザ
表示
コンテンツ
再生
リスト
オーディオ・
コントロール
メタデータ・
コントロール
メタデータ
表示

【図19】


1512
変化するオブジェクト
1501
プレイヤ・オブジェクト・マネージャ
1502
データ管理
1504
コピー／
再生管理
1506
圧縮解除
1503
ライブラリ
・アクセス
1505
非暗号化
1507
再 生
1508
アプリケーション間通信
ディジタル
・コンテンツ・
ライブラリ
196
191, 198
ウェブ・ブラウザ、
ヘルパ・アプリケーション
など

【図21】


新規コンテンツ要求
802
自動メタデータ獲得
803
161
メタデータ同化および入力ツール
手動メタデータ入力
804
使用条件
805
ウォーターマーキング
808
前処理および圧縮
809
155
コンテンツ処理ツール
品質管理
1704
暗号化
811
コンテンツSC作成
812
メタデータSC作成
807
コンテンツ散布
814